PCT/JP99/05689

14.10.99

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

EKJ

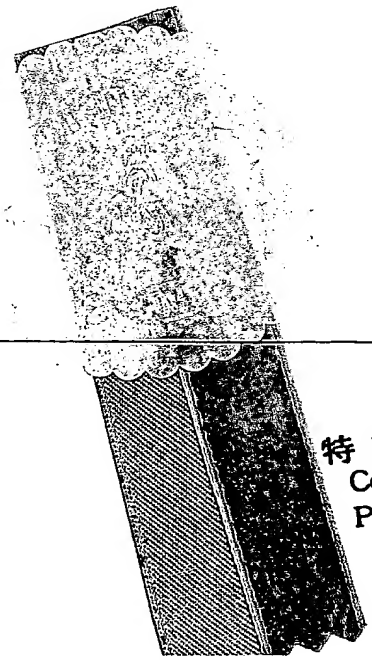
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 1999年 4月 9日

出願番号
Application Number: 平成11年特許願第103337号

出願人
Applicant (s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a)OR(b)



1999年 8月24日

特許庁長官
Commissioner,
Patent Office 伊佐山建志

出証番号 出証特平11-3(

【書類名】　特許願

【整理番号】　9900015013

【提出日】　平成11年 4月 9日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 12/16

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　松山　科子

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　石橋　義人

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　浅野　智之

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　北村　出

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　北原　淳

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100082131

【弁理士】

【氏名又は名称】　稲本　義雄

【電話番号】　03-3369-6479

【先の出願に基づく優先権主張】

【出願番号】　平成10年特許願第293829号

【出願日】　平成10年10月15日

【手数料の表示】

【予納台帳番号】　032089

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9708842

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　管理装置および方法、情報処理装置および方法、提供媒体、並びに情報利用システム

【特許請求の範囲】

【請求項１】　暗号化された情報を提供する情報提供装置、および前記情報を利用する情報処理装置を管理する管理装置において、

前記情報処理装置のIDおよびそのIDに対応して登録の可否を示すデータを有し、前記情報処理装置のIDを基に、前記情報処理装置を登録する登録手段

を備えることを特徴とする管理装置。

【請求項２】　前記データは、前記IDに対応して決済の可否を示すデータを含む

ことを特徴とする請求項１に記載の管理装置。

【請求項３】　前記登録手段は、前記管理装置と通信する前記情報処理装置に従属する他の情報処理装置を登録する

ことを特徴とする請求項１に記載の管理装置。

【請求項４】　暗号化された情報を提供する情報提供装置、および前記情報を利用する情報処理装置を管理する管理方法において、

前記情報処理装置のIDおよびそのIDに対応して登録の可否を示すデータを有し、前記情報処理装置のIDを基に、前記情報処理装置を登録する登録ステップ

を含むことを特徴とする管理方法。

【請求項５】　暗号化された情報を提供する情報提供装置、および前記情報を利用する情報処理装置を管理する管理装置に、

前記情報処理装置のIDおよびそのIDに対応して登録の可否を示すデータを有し、前記情報処理装置のIDを基に、前記情報処理装置を登録する登録ステップ

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項６】　管理装置に登録され、情報提供装置から提供される暗号化された情報を利用する情報処理装置において、

前記情報処理装置に従属する他の情報処理装置の登録を請求する登録請求手段

を備えることを特徴とする情報処理装置。

【請求項７】　前記情報処理装置は、前記情報処理装置に従属する他の情報処理装置の決済処理を代行する決済代行手段

を更に備えることを特徴とする請求項６に記載の情報処理装置。

【請求項８】　管理装置に登録され、情報提供装置から提供される暗号化された情報を利用する情報処理装置の情報処理方法において、

前記情報処理装置に従属する他の情報処理装置の登録を請求する登録請求ステップ

を含むことを特徴とする情報処理方法。

【請求項９】　管理装置に登録され、情報提供装置から提供される暗号化された情報を利用する情報処理装置に、

前記情報処理装置に従属する他の情報処理装置の登録を請求する登録請求ステップ

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項１０】　暗号化されて提供される情報を復号し、利用する情報処理装置、および前記情報処理装置を管理する管理装置からなる情報利用システムにおいて、

前記管理装置は、

前記情報処理装置のIDおよびそのIDに対応して登録の可否を示すデータを有し、前記情報処理装置のIDを基に、前記情報処理装置を登録する登録手段

を備え、

前記情報処理装置は、

前記情報処理装置に従属する他の情報処理装置の登録を請求する登録請求手段

を備えることを特徴とする情報利用システム。

【請求項１１】　管理装置に管理され、かつ、他の情報処理装置と接続され、暗号化された情報を復号し、利用する情報処理装置において、

前記管理装置および前記他の情報処理装置と相互認証する相互認証手段と、

所定の情報を復号する復号化手段と、

前記管理装置により作成された登録条件を授受する授受手段と、

前記授受手段により授受された前記登録条件を記憶する記憶手段と、

前記記憶手段により記憶されている前記登録条件に基づいて、動作を制御する制御手段と

を備えることを特徴とする情報処理装置。

【請求項１２】　管理装置に管理され、かつ、他の情報処理装置と接続され、暗号化された情報を復号し、利用する情報処理装置の情報処理方法において、

前記管理装置および前記他の情報処理装置と相互認証する相互認証ステップと、

所定の情報を復号する復号化ステップと、

前記管理装置により作成された登録条件を授受する授受ステップと、

前記授受ステップで授受された前記登録条件を記憶する記憶ステップと、

前記記憶ステップで記憶された前記登録条件に基づいて、動作を制御する制御ステップと

を含むことを特徴とする情報処理方法。

【請求項１３】　管理装置に管理され、かつ、他の情報処理装置と接続され、暗号化された情報を復号し、利用する情報処理装置に、

前記管理装置および前記他の情報処理装置と相互認証する相互認証ステップと、

所定の情報を復号する復号化ステップと、

前記管理装置により作成された登録条件を授受する授受ステップと、

前記授受ステップで授受された前記登録条件を記憶する記憶ステップと、

前記記憶ステップで記憶された前記登録条件に基づいて、動作を制御する制御ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項１４】　暗号化された情報を復号し、利用する情報処理装置を管理する管理装置において、

前記情報処理装置に供給するデータを暗号化する暗号手段と、

前記情報処理装置から、登録条件が送信されてきたとき、所定の処理を実行する実行手段と、

前記実行手段により所定の処理を実行するとき、前記情報処理装置の登録条件を作成する作成手段と、

前記作成手段により作成された前記登録条件を前記情報処理装置に送信する送信手段と

を備えることを特徴とする管理装置。

【請求項１５】　暗号化された情報を復号し、利用する情報処理装置を管理する管理装置の管理方法において、

前記情報処理装置に供給するデータを暗号化する暗号ステップと、

前記情報処理装置から、登録条件が送信されてきたとき、所定の処理を実行する実行ステップと、

前記実行ステップで所定の処理を実行するとき、前記情報処理装置の登録条件を作成する作成ステップと、

前記作成ステップで作成された前記登録条件を前記情報処理装置に送信する送信ステップと

を含むことを特徴とする管理方法。

【請求項１６】　暗号化された情報を復号し、利用する情報処理装置を管理する管理装置に、

前記情報処理装置に供給するデータを暗号化する暗号ステップと、

前記情報処理装置から、登録条件が送信されてきたとき、所定の処理を実行する実行ステップと、

前記実行ステップで所定の処理を実行するとき、前記情報処理装置の登録条件を作成する作成ステップと、

前記作成ステップで作成された前記登録条件を前記情報処理装置に送信する送信ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、管理装置および方法、情報処理装置および方法、提供媒体、並びに情報利用システムに関し、特に、暗号化された情報を復号する管理装置および方法、情報処理装置および方法、提供媒体、並びに情報利用システムに関する。

【０００２】

【従来の技術】

音楽などの情報を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザは、その情報処理装置で情報を復号して、再生するシステムがある。ユーザは、複数の情報処理装置で、情報を受信し、利用することができる。

【０００３】

【発明が解決しようとする課題】

ユーザは、契約のために、所定の手続をせねばならず、情報の提供者は、契約を要求するユーザの契約の可否を調査しなければならず、手間がかかり、契約成立までに時間がかかる課題があった。また、情報の提供者は、契約したユーザが不正を行った場合、それを発見するのが困難である課題があった。

【０００４】

また、複数の情報処理装置を有するユーザは、それぞれの情報処理装置毎に、契約し、利用料金を精算しなければならず、手間がかかる課題があった。

【０００５】

本発明はこのような状況に鑑みてなされたものであり、ユーザが簡単に情報提供の契約ができ、提供者も迅速にユーザの契約の可否が判断できることができるとともに、契約したユーザの不正行為や授受される情報の正当性を容易に確認することができるようにすることを目的とする。

【０００６】

【課題を解決するための手段】

請求項１に記載の管理装置は、情報処理装置のIDおよびそのIDに対応して登録の可否を示すデータを有し、情報処理装置のIDを基に、情報処理装置を登録する

登録手段を備えることを特徴とする。

【０００７】

請求項４に記載の管理方法は、情報処理装置のIDおよびそのIDに対応して登録の可否を示すデータを有し、情報処理装置のIDを基に、情報処理装置を登録する登録ステップを含むことを特徴とする。

【０００８】

請求項５に記載の提供媒体は、管理装置に、情報処理装置のIDおよびそのIDに対応して登録の可否を示すデータを有し、情報処理装置のIDを基に、情報処理装置を登録する登録ステップを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【０００９】

請求項６に記載の情報処理装置は、情報処理装置に従属する他の情報処理装置の登録を請求する登録請求手段を備えることを特徴とする。

【００１０】

請求項８に記載の情報処理方法は、情報処理装置に従属する他の情報処理装置の登録を請求する登録請求ステップを含むことを特徴とする。

【００１１】

請求項９に記載の提供媒体は、情報処理装置に、情報処理装置に従属する他の情報処理装置の登録を請求する登録請求ステップを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【００１２】

請求項１０に記載のシステムは、管理装置が、情報処理装置のIDおよびそのIDに対応して登録の可否を示すデータを有し、情報処理装置のIDを基に、情報処理装置を登録する登録手段を備え、情報処理装置が、情報処理装置に従属する他の情報処理装置の登録を請求する登録請求手段を備えることを特徴とする。

【００１３】

請求項１に記載の管理装置、請求項４に記載の管理方法、および請求項５に記載の提供媒体においては、情報処理装置のIDおよびそのIDに対応して登録の可否を示すデータを有し、情報処理装置のIDを基に、情報処理装置を登録する。

【００１４】

請求項６に記載の情報処理装置、請求項８に記載の情報処理方法、および請求項９に記載の提供媒体においては、情報処理装置に従属する他の情報処理装置の登録を請求する。

【００１５】

請求項１０に記載のシステムにおいては、管理装置が、情報処理装置のIDおよびそのIDに対応して登録の可否を示すデータを有し、情報処理装置のIDを基に、情報処理装置を登録し、情報処理装置が、情報処理装置に従属する他の情報処理装置の登録を請求する。

【００１６】

請求項１１に記載の情報処理装置は、管理装置および他の情報処理装置と相互認証する相互認証手段と、所定の情報を復号する復号化手段と、管理装置により作成された登録条件を授受する授受手段と、授受手段により授受された登録条件を記憶する記憶手段と、記憶手段により記憶されている登録条件に基づいて、動作を制御する制御手段とを備えることを特徴とする。

【００１７】

請求項１２に記載の情報処理方法は、管理装置および他の情報処理装置と相互認証する相互認証ステップと、所定の情報を復号する復号化ステップと、管理装置により作成された登録条件を授受する授受ステップと、授受ステップで授受された登録条件を記憶する記憶ステップと、記憶ステップで記憶された登録条件に基づいて、動作を制御する制御ステップとを含むことを特徴とする。

【００１８】

請求項１３に記載の提供媒体は、管理装置および他の情報処理装置と相互認証する相互認証ステップと、所定の情報を復号する復号化ステップと、管理装置により作成された登録条件を授受する授受ステップと、授受ステップで授受された登録条件を記憶する記憶ステップと、記憶ステップで記憶された登録条件に基づいて、動作を制御する制御ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【００１９】

請求項１１に記載の情報処理装置、請求項１２に記載の情報処理方法、および請求項１３に記載の提供媒体においては、管理装置および他の情報処理装置と相互認証され、所定の情報が暗号化され、管理装置により作成された登録条件が授受され、授受された登録条件が記憶され、記憶された登録条件に基づいて、動作が制御される。

【００２０】

請求項１４に記載の管理装置は、情報処理装置に供給するデータを暗号化する暗号手段と、情報処理装置から、登録条件が送信されてきたとき、所定の処理を実行する実行手段と、実行手段により所定の処理を実行するとき、情報処理装置の登録条件を作成する作成手段と、作成手段により作成された登録条件を情報処理装置に送信する送信手段とを備えることを特徴とする。

【００２１】

請求項１５に記載の管理方法は、情報処理装置に供給するデータを暗号化する暗号ステップと、情報処理装置から、登録条件が送信されてきたとき、所定の処理を実行する実行ステップと、実行ステップで所定の処理を実行するとき、情報処理装置の登録条件を作成する作成ステップと、作成ステップで作成された登録条件を情報処理装置に送信する送信ステップとを含むことを特徴とする。

【００２２】

請求項１６に記載の提供媒体は、情報処理装置に供給するデータを暗号化する暗号ステップと、情報処理装置から、登録条件が送信されてきたとき、所定の処理を実行する実行ステップと、実行ステップで所定の処理を実行するとき、情報処理装置の登録条件を作成する作成ステップと、作成ステップで作成された登録条件を情報処理装置に送信する送信ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【００２３】

請求項１４に記載の管理装置、請求項１５に記載の管理方法、および請求項１６に記載の提供媒体においては、情報処理装置に供給するデータが復され、情報処理装置から、登録条件が送信されてきたとき、所定の処理が実行され、所定の処理が実行されるとき、情報処理装置の登録条件が作成され、作成された登録条

件が情報処理装置に送信される。

【００２４】

【発明の実施の形態】

以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【００２５】

図１は、本発明を適用したEMD(Electronic Music Distribution:電子音楽配信)システムを説明する図である。このシステムでユーザに配信されるコンテンツ(Content)とは、情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。EMDサービスセンタ１は、コンテンツプロバイダ２、ユーザホームネットワーク５等に配送用鍵Ｋｄを送信し、ユーザホームネットワーク５から、コンテンツの利用に応じた課金情報等を受信し、利用料金を精算し、コンテンツプロバイダ２およびサービスプロバイダ３への利益分配の処理を行う。

【００２６】

コンテンツプロバイダ２は、デジタル化されたコンテンツを有し、自己のコンテンツであることを証明するためのウォータマーク（電子透かし）をコンテンツに挿入し、コンテンツを圧縮し、および暗号化し、所定の情報を付加して、サービスプロバイダ３に送信する。

【００２７】

サービスプロバイダ３は、専用のケーブルネットワーク、インターネット、または衛星などから構成されるネットワーク４を介して、コンテンツプロバイダ２から供給されたコンテンツに価格を付して、ユーザホームネットワーク５に送信する。

【００２８】

ユーザホームネットワーク５は、サービスプロバイダ３から価格を付して送付

されたコンテンツを入手し、コンテンツを復号、再生して利用するとともに課金処理を実行する。課金処理により得られた課金情報は、ユーザホームネットワーク５が配送用鍵Ｋｄを EMDサービスセンタ１から入手する際、EMDサービスセンタ１に送信される。

【００２９】

図２は、EMDサービスセンタ１の機能の構成を示すブロック図である。サービスプロバイダ管理部１１は、サービスプロバイダ３に利益分配の情報を供給するとともに、コンテンツプロバイダ２から供給されるコンテンツに付される情報（取扱方針）が暗号化されている場合、サービスプロバイダ３に配送用鍵Ｋｄを送信する。コンテンツプロバイダ管理部１２は、コンテンツプロバイダ２に配送用鍵Ｋｄを送信するとともに、利益分配の情報を供給する。著作権管理部１３は、ユーザホームネットワーク５のコンテンツの利用の実績を示す情報を、著作権を管理する団体、例えば、JASRAC(Japanese Society for Rights of Authors,Composers and Publishers:日本音楽著作権協会)に送信する。鍵サーバ１４は、配送用鍵Ｋｄを記憶しており、コンテンツプロバイダ管理部１２、またはユーザ管理部１８等を介して、配送用鍵Ｋｄをコンテンツプロバイダ２、またはユーザホームネットワーク５等に供給する。ユーザ管理部１８は、ユーザホームネットワーク５のコンテンツの利用の実績を示す情報である課金情報、そのコンテンツに対応する価格情報、およびそのコンテンツに対応する取扱方針を入力し、経歴データ管理部１５に記憶させる。

【００３０】

EMDサービスセンタ１からコンテンツプロバイダ２およびユーザホームネットワーク５を構成するレシーバ５１（図１０で後述する）への、配送用鍵Ｋｄの定期的な送信の例について、図３乃至図６を参照に説明する。図３は、コンテンツプロバイダ２がコンテンツの提供を開始し、ユーザホームネットワーク５を構成するレシーバ５１がコンテンツの利用を開始する、１９９８年１月における、EMDサービスセンタ１が有する配送用鍵Ｋｄ、コンテンツプロバイダ２が有する配送用鍵Ｋｄ、およびレシーバ５１が有する配送用鍵Ｋｄを示す図である。

【００３１】

図３の例において、配送用鍵Ｋｄは、暦の月の初日から月の末日まで、使用可能であり、たとえば、所定のビット数の乱数である”ａａａａａａａａ”の値を有するバージョン１である配送用鍵Ｋｄは、１９９８年１月１日から１９９８年１月３１日まで使用可能（すなわち、１９９８年１月１日から１９９８年１月３１日の期間にサービスプロバイダ３がユーザホームネットワーク５に配布するコンテンツを暗号化するコンテンツ鍵Ｋｃｏは、バージョン１である配送用鍵Ｋｄで暗号化されている）であり、所定のビット数の乱数である”ｂｂｂｂｂｂｂｂ”の値を有するバージョン２である配送用鍵Ｋｄは、１９９８年２月１日から１９９８年２月２８日まで使用可能（すなわち、その期間にサービスプロバイダ３がユーザホームネットワーク５に配布するコンテンツを暗号化するコンテンツ鍵Ｋｃｏは、バージョン２である配送用鍵Ｋｄで暗号化されている）である。同様に、バージョン３である配送用鍵Ｋｄは、１９９８年３月中に使用可能であり、バージョン４である配送用鍵Ｋｄは、１９９８年４月中に使用可能であり、バージョン５である配送用鍵Ｋｄは、１９９８年５月中に使用可能であり、バージョン６である配送用鍵Ｋｄは、１９９８年６月中に使用可能である。

【００３２】

コンテンツプロバイダ２がコンテンツの提供を開始するに先立ち、EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年１月から１９９８年６月まで利用可能な、バージョン１乃至バージョン６の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、記憶する。６月分の配送用鍵Ｋｄを記憶するのは、コンテンツプロバイダ２は、コンテンツを提供する前のコンテンツおよびコンテンツ鍵の暗号化などの準備に、所定の期間が必要だからである。

【００３３】

また、レシーバ５１がコンテンツの利用を開始するに先立ち、EMDサービスセンタ１は、レシーバ５１に、１９９８年１月から１９９８年３月まで、利用可能なバージョン１乃至バージョン３である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、記憶する。３月分の配送用鍵Ｋｄを記憶するのは、レシーバ５１が、EMDサービスセンタ１に接続できないなどのトラブ

ルにより、コンテンツの利用が可能な契約期間にもかかわらずコンテンツが利用できない等の事態を避けるためであり、また、EMDサービスセンタ１への接続の頻度を低くし、ユーザホームネットワーク５の負荷を低減するためである。

【００３４】

１９９８年１月１日から１９９８年１月３１日の期間には、バージョン１である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００３５】

１９９８年２月１日における、EMDサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図４で説明する。EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年２月から１９９８年７月まで利用可能な、バージョン２乃至バージョン７の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、レシーバ５１に、１９９８年２月から１９９８年４月まで、利用可能なバージョン２乃至バージョン４である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、バージョン１である配送用鍵Ｋｄをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送用鍵Ｋｄを利用できるようにするためである。

【００３６】

１９９８年２月１日から１９９８年２月２８日の期間には、バージョン２である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００３７】

１９９８年３月１日における、EMDサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図５で説明する。EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年３月から１９９８年８月

まで利用可能な、バージョン３乃至バージョン８の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、レシーバ５１に、１９９８年３月から１９９８年５月まで、利用可能なバージョン３乃至バージョン５である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、バージョン１である配送用鍵ＫｄおよびバージョンＮ２である配送用鍵Ｋｄをそのまま記憶する。

【００３８】

１９９８年３月１日から１９９８年３月３１日の期間には、バージョン３である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００３９】

１９９８年４月１日における、EMDサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図６で説明する。EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年４月から１９９８年９月まで利用可能な、バージョン４乃至バージョン９の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、レシーバ５１に、１９９８年４月から１９９８年６月まで、利用可能なバージョン４乃至バージョン６である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、バージョン１である配送用鍵Ｋｄ、バージョン２である配送用鍵Ｋｄ、およびバージョン３である配送用鍵Ｋｄをそのまま記憶する。

【００４０】

１９９８年４月１日から１９９８年４月３０日の期間には、バージョン４である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホ

ームネットワーク５を構成するレシーバ５１で利用される。

【００４１】

このように、あらかじめ先の月の配送用鍵Ｋｄを配布しておくことで、仮にユーザーが１，２ヶ月まったくセンターにアクセスしていなくても、一応、コンテンツの買い取りが行え、時を見計らって、センターにアクセスして鍵を受信することができる。

【００４２】

利益分配部１６は、経歴データ管理部１５から供給された、課金情報、価格情報、および取扱方針に基づき、EMDサービスセンタ１、コンテンツプロバイダ２、およびサービスプロバイダ３の利益を算出する。相互認証部１７は、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５の所定の機器と後述する相互認証を実行する。

【００４３】

ユーザ管理部１８は、ユーザ登録データベースを有し、ユーザホームネットワーク５の機器から登録の要求があったとき、ユーザ登録データベースを検索し、その記録内容に応じて、その機器を登録したり、または登録を拒絶する等の処理を実行する。ユーザホームネットワーク５がEMDサービスセンタ１と接続が可能な機能を有する複数の機器から構成されているとき、ユーザ管理部１８は、登録が可能か否かの判定の処理の結果に対応して、決済をする機器を指定し、さらに、コンテンツの利用条件を規定した登録リストをユーザホームネットワーク５の所定の機器に送信する。

【００４４】

図７に示すユーザ登録データベースの例は、ユーザホームネットワーク５の機器の機器固有の６４ビットからなるID（Identification Data）を記録し、そのIDに対応して（すなわち、そのIDを有する機器毎に）、決済処理が可能か否か、登録が可能か否か、EMDサービスセンタ１と接続が可能か否か等の情報を記録する。ユーザ登録データベースに記録された登録が可能か否かの情報は、決済機関（例えば、銀行）、またはサービスプロバイダ３などから供給される料金の未払い、不正処理等の情報を基に、所定の時間間隔で更新される。登録が不可と記録

されたIDを有する機器の登録の要求に対して、ユーザ管理部１８は、その登録を拒否し、登録を拒否された機器は、以後、このシステムのコンテンツを利用できない。

【００４５】

ユーザ登録データベースに記録された決済処理が可能か否かの情報は、その機器が、決済可能か否かを示す。ユーザホームネットワーク５が、コンテンツの再生またはコピーなどの利用が可能な複数の機器で構成されているとき、その中の決済処理が可能である１台の機器は、EMDサービスセンタ１に、ユーザホームネットワーク５のEMDサービスセンタ１に登録されている全ての機器の、課金情報、価格情報、および取扱方針を出力する。ユーザ登録データベースに記録されたEMDサービスセンタ１と接続が可能か否かの情報は、その機器が、EMDサービスセンタ１と接続が可能であるか否かを示し、接続ができないと記録された機器は、ユーザホームネットワーク５の他の機器を介して、EMDサービスセンタ１に、課金情報等を出力する。

【００４６】

また、ユーザ管理部１８は、ユーザホームネットワーク５の機器から課金情報、価格情報、および取扱方針が供給され、その情報を経歴データ管理部１５に出力し、さらに、所定の処理（タイミング）で、ユーザホームネットワーク５の機器に、配送用鍵Ｋｄを供給する。

【００４７】

課金請求部１９は、経歴データ管理部１５から供給された、課金情報、価格情報、および取扱方針に基づき、ユーザへの課金を算出し、その結果を、出納部２０に供給する。出納部２０は、ユーザ、コンテンツプロバイダ２、およびサービスプロバイダ３への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決算処理を実行する。監査部２１は、ユーザホームネットワーク５の機器から供給された課金情報、価格情報、および取扱方針の正当性（すなわち、不正をしていないか）を監査する。

【００４８】

図８は、コンテンツプロバイダ２の機能の構成を示すブロック図である。コン

テンツサーバ３１は、ユーザに供給するコンテンツを記憶し、ウォータマーク付加部３２に供給する。ウォータマーク付加部３２は、コンテンツサーバ３１から供給されたコンテンツにウォータマークを付加し、圧縮部３３に供給する。圧縮部３３は、ウォータマーク付加部３２から供給されたコンテンツを、ATRAC2(Adaptive Transform Acoustic Coding 2)（商標）等の方式で圧縮し、暗号化部３４に供給する。暗号化部３４は、圧縮部３３で圧縮されたコンテンツを、乱数発生部３５から供給された乱数を鍵（以下、この乱数をコンテンツ鍵Ｋｃｏと称する）として、DES(Data Encryption Standard)などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部３８に出力する。

【００４９】

乱数発生部３５は、コンテンツ鍵Ｋｃｏとなる所定のビット数の乱数を暗号化部３４および暗号化部３６に供給する。暗号化部３６は、コンテンツ鍵ＫｃｏをEMDサービスセンタ１から供給された配送用鍵Ｋｄを使用して、DESなどの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部３８に出力する。

【００５０】

DESは、５６ビットの共通鍵を用い、平文の６４ビットを１ブロックとして処理する暗号方式である。DESの処理は、平文を攪拌し、暗号文に変換する部分（データ攪拌部）と、データ攪拌部で使用する鍵（拡大鍵）を共通鍵から生成する部分（鍵処理部）からなる。DESのすべてのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

【００５１】

まず、平文の６４ビットは、上位３２ビットのH_0、および下位３２ビットのL_0に分割される。鍵処理部から供給された４８ビットの拡大鍵K_1、および下位３２ビットのL_0を入力とし、下位３２ビットのL_0を攪拌したＦ関数の出力が算出される。Ｆ関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の２種類の基本変換から構成されている。次に、上位３２ビットのH_0と、Ｆ関数の出力が排他的論理和され、その結果はL_1とされる。L_0は、H_1とされる。

【００５２】

上位３２ビットのH_0および下位３２ビットのL_0を基に、以上の処理を１６回繰り返し、得られた上位３２ビットのH_{16}および下位３２ビットのL_{16}が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

【００５３】

ポリシー記憶部３７は、コンテンツの取扱方針（ポリシー）を記憶し、暗号化されるコンテンツに対応して、取扱方針をセキュアコンテナ作成部３８に出力する。セキュアコンテナ作成部３８は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、並びに暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、および取扱方針のハッシュ値をとり作成された署名、さらにコンテンツプロバイダ２の公開鍵Ｋｐｃｐを含む証明書から構成されるコンテンツプロバイダセキュアコンテナを作成し、サービスプロバイダ３に供給する。相互認証部３９は、EMDサービスセンタ１から配送用鍵Ｋｄの供給を受けるのに先立ち、EMDサービスセンタ１と相互認証し、また、サービスプロバイダ３へのコンテンツプロバイダセキュアコンテナの送信に先立ち、サービスプロバイダ３と相互認証する。

【００５４】

署名は、データまたは後述する証明書に付け、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵で暗号化して作成される。

【００５５】

ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの１ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

【００５６】

署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その

結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、MD4，MD5，SHA-1などが用いられる。

【００５７】

次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

【００５８】

公開鍵暗号の中で代表的なRSA（Rivest-Shamir-Adleman）暗号を、簡単に説明する。まず、２つの十分に大きな素数であるpおよびqを求め、さらにpとqの積であるｎを求める。(p-1)と(q-1)の最小公倍数Lを算出し、更に、３以上L未満で、かつ、Ｌと互いに素な数eを求める（すなわち、eとLを共通に割り切れる数は、１のみである）。

【００５９】

次に、Lを法とする乗算に関するeの乗法逆元dを求める。すなわち、d，e、およびLの間には、ed=1 mod Lが成立し、dはユークリッドの互除法で算出できる。このとき、nとeが公開鍵とされ、p,q,およびdが、秘密鍵とされる。

【００６０】

暗号文Cは、平文Mから、式（１）の処理で算出される。

【００６１】

$$C=M^e \bmod n \quad (1)$$

暗号文Cは、式（２）の処理で平文Mに、復号される。

【００６２】

$$M=C^d \bmod n \quad (2)$$

証明は省略するが、RSA暗号で平文を暗号文に変換して、それが復号できるのは、フェルマーの小定理に根拠をおいており、式（３）が成立するからである。

【００６３】

M=C^d=(M^e)^d=M^(ed)= mod n　（３）

秘密鍵pとqを知っているならば、公開鍵eから秘密鍵dは算出できるが、公開鍵nの素因数分解が計算量的に困難な程度に公開鍵nの桁数を大きくすれば、公開鍵nを知るだけでは、公開鍵eから秘密鍵dは計算できず、復号できない。以上のように、RSA暗号では、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【００６４】

また、公開鍵暗号の他の例である楕円曲線暗号についても、簡単に説明する。楕円曲線y^2=x^3+ax+b上の、ある点をBとする。楕円曲線上の点の加算を定義し、nBは、Bをn回加算した結果を表す。同様に、減算も定義する。BとnBからnを算出することは、困難であることが証明されている。BとnBを公開鍵とし、nを秘密鍵とする。乱数rを用いて、暗号文C1およびC2は、平文Mから、公開鍵で式（４）および式（５）の処理で算出される。

【００６５】

C1=M+rnB　（４）

C2=rB　（５）

暗号文C1およびC2は、式（６）の処理で平文Mに、復号される。

【００６６】

M=C1-nC2　（６）

復号できるのは、秘密鍵nを有するものだけである。以上のように、RSA暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【００６７】

図９は、サービスプロバイダ３の機能の構成を示すブロック図である。コンテンツサーバ４１は、コンテンツプロバイダ２から供給された、暗号化されているコンテンツを記憶し、セキュアコンテナ作成部４４に供給する。値付け部４２は

、コンテンツに対応した取扱方針を基に、価格情報を作成し、セキュアコンテナ作成部４４に供給する。ポリシー記憶部４３は、コンテンツプロバイダ２から供給された、コンテンツの取扱方針を記憶し、セキュアコンテナ作成部４４に供給する。相互認証部４５は、コンテンツプロバイダ２からコンテンツプロバイダセキュアコンテナの供給を受け取るのに先立ち、コンテンツプロバイダ２と相互認証し、また、ユーザホームネットワーク５へのサービスプロバイダセキュアコンテナの送信に先立ち、ユーザホームネットワーク５と相互認証する。また、コンテンツプロバイダ２が取扱方針を配送用鍵Ｋｄで暗号化して供給する場合、相互認証部４５は、EMDサービスセンタ１から配送用鍵Ｋｄの供給を受け付けるのに先立ち、EMDサービスセンタ１と相互認証する。

【００６８】

図１０は、ユーザホームネットワーク５の構成を示すブロック図である。レシーバ５１は、ネットワーク４を介して、サービスプロバイダ３からコンテンツを含んだサービスプロバイダセキュアコンテナを受信し、コンテンツを復号および伸張し、再生する。

【００６９】

通信部６１は、ネットワーク４を介してサービスプロバイダ３、またはEMDサービスセンタ１と通信し、所定の情報を受信し、または送信する。SAM(Secure Application Module)６２は、サービスプロバイダ３、またはEMDサービスセンタ１と相互認証し、コンテンツの暗号を復号し、またはコンテンツを暗号化し、さらに配送用鍵Ｋｄ等を記憶する。伸張部６３は、コンテンツの暗号を復号し、ATRAC2方式で伸張し、さらに所定のウォータマークをコンテンツに挿入する。IC（Integrated Circuit）カードインターフェース６４は、SAM６２からの信号を所定の形式に変更し、レシーバ５１に装着されたICカード５５に出力し、また、ICカード５５からの信号を所定の形式に変更し、SAM６２に出力する。

【００７０】

サービスプロバイダ３、またはEMDサービスセンタ１と相互認証し、課金処理を実行し、コンテンツ鍵Ｋｃｏを復号および暗号化し、さらに使用許諾条件情報等の所定のデータを記憶するSAM６２は、相互認証モジュール７１、課金モジュ

ール７２、記憶モジュール7_3、および復号／暗号化モジュール７４から構成される。このSAM６２は、シングルチップの暗号処理専用ICで構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパー性）を有する。

【００７１】

相互認証モジュール７１は、サービスプロバイダ３、またはEMDサービスセンタ１との相互認証を実行し、必要に応じて、一時鍵Ｋｔｅｍｐ（セッション鍵）を復号／暗号化モジュール７４に供給する。課金処理モジュール７２は、サービスプロバイダ３から受信したサービスプロバイダセキュアコンテナに含まれる取扱方針および価格情報（並びに、場合によっては、取扱制御情報）から、使用許諾条件情報および課金情報を生成し、記憶モジュール７３またはHDD(Hard Disk Drive)５２に出力する。記憶モジュール７３は、課金処理モジュール７２または復号／暗号化モジュール７４から供給された課金情報、および配送用鍵Ｋｄ等のデータを記憶し、他の機能ブロックが所定の処理を実行するとき、配送用鍵Ｋｄ等のデータを供給する。

【００７２】

復号／暗号化モジュール７４は、復号ユニット９１、乱数発生ユニット９２、および暗号化ユニット９３から構成される。復号ユニット９１は、暗号化されたコンテンツ鍵Ｋｃｏを配送用鍵Ｋｄで復号し、暗号化ユニット９３に出力する。乱数発生ユニット９２は、相互認証時に、所定の桁数の乱数を発生し、必要に応じて一時鍵Ｋｔｅｍｐを生成し、暗号化ユニット９３に出力する。暗号化ユニット９３は、復号されたコンテンツ鍵Ｋｃｏを、再度、記憶モジュール７３に保持された保存用鍵Ｋｓａｖｅで暗号化し、HDD５２に出力する。暗号化ユニット９３は、コンテンツ鍵Ｋｃｏを伸張部６３に送信するとき、コンテンツ鍵Ｋｃｏを乱数発生ユニット９２で生成した一時鍵Ｋｔｅｍｐで暗号化する。

【００７３】

コンテンツを復号し、伸張し、所定のウォータマークを付加する伸張部６３は、相互認証モジュール７５、復号モジュール７６、復号モジュール７７、伸張モ

ジュール７８、およびウォータマーク付加モジュール７９から構成される。相互認証モジュール７５は、SAM６２と相互認証し、一時鍵Ｋｔｅｍｐを復号モジュール７６に出力する。復号モジュール７６は、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号し、復号モジュール７７に出力する。復号モジュール７７は、HDD５２に記録された、保存用鍵Ｋｓａｖｅで暗号化されているコンテンツを、記憶モジュール７３に記憶されている保存用鍵Ｋｓａｖｅでコンテンツ鍵Ｋｃｏで復号し、伸張モジュール７８に出力する。伸張モジュール７８は、復号されたコンテンツを、更にATRAC2等の方式で伸張し、ウォータマーク付加モジュール７９に出力する。ウォータマーク付加モジュール７９は、コンテンツにレシーバ５１を特定する所定のウォータマークを挿入し、レコーダ５３に出力したり、図示せぬスピーカに出力し、音楽を再生する。

【００７４】

HDD５２は、サービスプロバイダ３から供給されたコンテンツを記録する。装着された光ディスク（図示せず）にサービスプロバイダ３から供給されたコンテンツを記録し、再生するレコーダ５３は、記録再生部６５、SAM６６、および伸張部６７から構成される。記録再生部６５は、光ディスクが装着され、その光ディスクにコンテンツを記録し、再生する。SAM６６は、SAM６２と同じ機能を有し、その説明は省略する。伸張部６７は、伸張部６３と同じ機能を有し、その説明は省略する。MD(Mini Disk:商標)ドライブ５４は、装着された図示せぬMDにサービスプロバイダ３から供給されたコンテンツを記録し、再生する。

【００７５】

ICカード５５は、レシーバ５１に装着され、記憶モジュール７３に記憶された配送用鍵Ｋｄおよび機器のIDなどの所定のデータを記憶する。例えば、新たなレシーバ５１を購入し、今まで使用していたレシーバ５１と入れ替えて使用する場合、まず、ユーザは、ICカード５５に、今まで使用していたレシーバ５１の記憶モジュール７３に記憶されていた配送用鍵Ｋｄなどの所定のデータを記憶させる。次に、ユーザは、そのICカード５５を新たなレシーバ５１に装着し、そのレシーバ５１を操作して、EMDサービスセンタ１のユーザ管理部１８にその新たなレシーバ５１を登録する。EMDサービスセンタ１のユーザ管理部１８は、ICカード

５５に記憶されていたデータ（今まで使用していたレシーバ５１のIDなど）を基に、ユーザ管理部１８が保持しているデータベースから、ユーザの氏名、使用料の払い込みに使用するクレジットカードの番号などのデータを検索し、そのデータを基に、登録の処理を実行するので、ユーザは、面倒なデータを入力する必要がない。ICカード５５は、相互認証モジュール８０および記憶モジュール８１で構成される。相互認証モジュール８０は、SAM６２と相互認証する。記憶モジュール８１は、ICカードインターフェース６４を介して、SAM６２から供給されたデータを記憶し、記憶したデータをSAM６２に出力する。

【００７６】

図１１は、ユーザホームネットワーク５の他の構成例を示すブロック図である。この構成のレシーバ５１およびレコーダ５３は、図１０に示した伸張部６３および伸張部６７を省略した構成を有する。その代わり、レコーダ５３に接続されているデコーダ５６が、伸張部６３または伸張部６７と同じ機能を有する。その他の構成は、図１０における場合と同様である。

【００７７】

コンテンツを復号し、伸張し、ウォータマークを付加するデコーダ５６は、相互認証モジュール１０１、復号モジュール１０２、復号モジュール１０３、伸張モジュール１０４、およびウォータマーク付加モジュール１０５から構成される。相互認証モジュール１０１は、SAM６２またはSAM６６と相互認証し、一時鍵Ｋｔｅｍｐを復号モジュール１０２に出力する。復号モジュール１０２は、SAM６２から出力され、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号し、復号モジュール１０３に出力する。復号モジュール１０３は、HDD５２に記録されたコンテンツをコンテンツ鍵Ｋｃｏで復号し、伸張モジュール１０４に出力する。伸張モジュール１０４は、復号されたコンテンツを、更にATRAC2等の方式で伸張し、ウォータマーク付加モジュール１０５に出力する。ウォータマーク付加モジュール１０５は、コンテンツにデコーダ５６を特定する所定のウォータマークを挿入し、レコーダ５３に出力したり、図示せぬスピーカに出力し、音楽を再生する。

【００７８】

図１２は、EMDサービスセンタ１、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５の間で送受信される情報を説明する図である。コンテンツプロバイダ２は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、および署名をコンテンツプロバイダセキュアコンテナ（その詳細は図１３を参照して後述する）に格納し、さらにコンテンツプロバイダセキュアコンテナにコンテンツプロバイダ２の証明書（その詳細は図１４を参照して後述する）を付して、サービスプロバイダ３に送信する。コンテンツプロバイダ２はまた、取扱方針、および署名にコンテンツプロバイダ２の証明書を付して、EMDサービスセンタ１に送信する。

【００７９】

サービスプロバイダ３は、受信したコンテンツプロバイダセキュアコンテナに含まれる取扱方針を基に価格情報を生成し、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、価格情報、および署名をサービスプロバイダセキュアコンテナ（その詳細は図１５を参照して後述する）に格納し、さらにサービスプロバイダセキュアコンテナにサービスプロバイダ３の証明書（その詳細は図１６を参照して後述する）を付して、ユーザホームネットワーク５に送信する。サービスプロバイダ３はまた、価格情報、および署名にサービスプロバイダ３の証明書を付して、EMDサービスセンタ１に送信する。

【００８０】

ユーザホームネットワーク５は、受信したサービスプロバイダセキュアコンテナに含まれる取扱方針から使用許諾条件情報を生成し、使用許諾条件情報に沿って、コンテンツを利用する。ユーザホームネットワーク５において、コンテンツ鍵Ｋｃｏが復号されると、課金情報が生成される。課金情報は、必要に応じ、所定のタイミングで、暗号化され、取扱方針および価格情報と共に署名が付され、EMDサービスセンタ１に送信される。

【００８１】

EMDサービスセンタ１は、課金情報および取扱方針を基に使用料金を算出し、またEMDサービスセンタ１、コンテンツプロバイダ２、およびサービスプロバイダ３それぞれの利益を算出する。EMDサービスセンタ１は、さらに、コンテンツ

プロバイダ２から受信した取扱方針、サービスプロバイダ３から受信した価格情報、並びにユーザホームネットワーク５から受信した課金情報、取扱方針、および価格情報を比較し、サービスプロバイダ３またはユーザホームネットワーク５で取扱方針の改竄または不正な価格の付加等の不正がなかったか否かを監査する。

【００８２】

図１３は、コンテンツプロバイダセキュアコンテナを説明する図である。コンテンツプロバイダセキュアコンテナは、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、および署名を含む。署名は、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、および取扱方針にハッシュ関数を適用して生成されたハッシュ値を、コンテンツプロバイダ２の秘密鍵Ｋｓｃｐで暗号化したデータである。

【００８３】

図１４は、コンテンツプロバイダ２の証明書を説明する図である。コンテンツプロバイダ２の証明書は、証明書のバージョン番号、認証局がコンテンツプロバイダ２に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、コンテンツプロバイダ２の名前、コンテンツプロバイダの公開鍵Ｋｐｃｐ、並びに署名を含む。署名は、証明書のバージョン番号、認証局がコンテンツプロバイダ２に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、コンテンツプロバイダ２の名前、並びにコンテンツプロバイダの公開鍵Ｋｐｃｐにハッシュ関数を適用して生成されたハッシュ値を、認証局の秘密鍵Ｋｓｃａで暗号化したデータである。

【００８４】

~~図１５は、サービスプロバイダセキュアコンテナを説明する図である。サービス~~プロバイダセキュアコンテナは、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、コンテンツプロバイダ２により作成された署名、価格情報、および署名を含む。署名は、コン

テンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、コンテンツプロバイダ２により作成された署名、および価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ３の秘密鍵Ｋｓｓｐで暗号化したデータである。

【００８５】

図１６は、サービスプロバイダ３の証明書を説明する図である。サービスプロバイダ３の証明書は、証明書のバージョン番号、認証局がサービスプロバイダ３に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ３の名前、サービスプロバイダの公開鍵Ｋｐｓｐ、並びに署名を含む。署名は、証明書のバージョン番号、認証局がサービスプロバイダ３に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ３の名前、サービスプロバイダの公開鍵Ｋｐｓｐにハッシュ関数を適用して生成されたハッシュ値を、認証局の秘密鍵Ｋｓｃａで暗号化したデータである。

【００８６】

図１７は、取扱方針、価格情報、および使用許諾条件情報を示す図である。コンテンツプロバイダ２が有する取扱方針（図１７（Ａ））は、コンテンツ毎に用意され、ユーザホームネットワーク５が利用可能な利用内容を示す。例えば、図１７（Ａ）の取り扱い方針は、ユーザホームネットワーク５がそのコンテンツを再生およびシングルコピーすることは許可するが、マルチコピーは許可しないことを示す。

【００８７】

図１８は、シングルコピーおよびマルチコピーを説明する図である。マルチコピーは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合において、そのコンテンツから、複数のコピーを作成することを言う。ただし、図１８（Ａ）に示すように、コピーを更にコピーすることはできない（許されない）。シングルコピーは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を

購入した場合において、そのコンテンツから、ただ１つのコピーを作成することを言う。シングルコピーの場合も、図１８（Ｂ）に示すように、コピーを更にコピーすることはできない（許されない）。

【００８８】

サービスプロバイダ３は、図１７（Ｂ）に示すように、コンテンツプロバイダ２からの取扱方針（図１７（Ａ））に価格情報を加える。例えば、図１７（Ｂ）の価格情報は、そのコンテンツを再生して利用するときの料金が１５０円で、マルチコピーして利用するときの利用料金が８０円であることを示す。図１７には、例示しないが、シングルコピーの価格情報は、コピーの１回当たりの使用料金を表し、例えば、３回のコピーの利用では、シングルコピーの使用料金の３倍の料金を支払う。マルチコピーまたはシングルコピーが許可されるコンテンツは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合における、そのコンテンツに限られる。

【００８９】

ユーザホームネットワーク５は、サービスプロバイダ３から供給される取扱方針が示すコンテンツの利用可能な利用内容（図１７（Ｂ））から、ユーザが選択した、利用内容を示す使用許諾条件情報（図１７（Ｃ））を記憶する。例えば、図１７（Ｃ）の使用許諾条件情報は、そのコンテンツを再生して使用することができ、シングルコピーおよびマルチコピーができないことを示す。

【００９０】

図１９は、図１７の例と比較してコンテンツプロバイダ２が取扱方針に利益分配の情報を加え、サービスプロバイダ３が価格情報に利益分配の情報を加える場合の、取扱方針および価格情報を説明する図である。図１７に示す例に対して、図１９の例では、コンテンツプロバイダ２の利益が、コンテンツを再生して利用するとき７０円で、マルチコピーして利用するとき４０円であることを示す情報が、追加されている（図１９（Ａ））。更に、利益分配情報として、サービスプロバイダ３の利益が、コンテンツを再生して利用するとき６０円で、マルチコピーして利用するとき３０円であることが、追加されている（図１９（Ｂ））。価格は、図１７（Ａ）における場合と同様に、再生が１５０円、マルチコピーが８

０円とされている。価格（例えば１５０円）からコンテンツプロバイダ２の利益（例えば７０円）およびサービスプロバイダ３の利益（例えば６０円）を差し引いた金額（例えば２０円）が、EMDサービスセンタ１の利益である。EMDサービスセンタ１は、ユーザホームネットワーク５のコンテンツの利用結果を示す課金情報（図１９（Ｃ））とともに、ユーザホームネットワーク５を介して、取扱方針、利益分配率、および価格情報を得ることで、コンテンツプロバイダ２、サービスプロバイダ３、およびEMDサービスセンタ１のそれぞれの利益を算出できる。

【００９１】

図２０は、コンテンツの再生の利用に、複数の形態が設定されているときの取扱方針、価格情報、および使用許諾条件情報を説明する図である。図２０（Ａ）の例では、サービスプロバイダ３において、取扱方針および価格情報として、コンテンツの再生利用に、制限のない再生、回数制限（この例の場合、５回）のある再生、および期日制限（この例の場合、１９９８年１２月３１日まで）のある再生が設定されている。ユーザが、５回の回数制限のある再生を選択して、コンテンツを利用する場合、コンテンツを受け取り、まだ１度も再生していない状態では、図２０（Ｂ）に示すように、ユーザホームネットワーク５の使用許諾条件情報の回数制限に対応する値には、”５”が記録されている。この回数制限に対応する値は、ユーザホームネットワーク５において、コンテンツが再生（利用）される度にデクリメントされ、例えば、３回再生された後、その値は、図２０（Ｃ）に示すように”２”とされる。回数制限に対応する値が、”０”となった場合、ユーザホームネットワーク５は、それ以上、そのコンテンツを再生して利用することができない。

【００９２】

図２１は、EMDサービスセンタ１、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５の間で送受信される情報の他の例を説明する図である。図１２に示した例に対して、図２１の例では、サービスプロバイダ３は、コンテンツプロバイダ２からの取扱方針を基に取扱制御情報を作成する。取扱制御情報は、コンテンツなどと共にサービスプロバイダセキュアコンテナに格納され、ユーザホームネットワーク５に送信され、EMDサービスセンタ

１にも送信される。取扱制御情報は、更に、課金情報および取扱方針と共にユーザホームネットワーク５からEMDサービスセンタ１に送信される。

【００９３】

図２２は、図２１の例の場合のサービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、コンテンツプロバイダ２により生成された署名、取扱制御情報、価格情報、および署名を含む。署名は、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、コンテンツプロバイダ２により生成された署名、取扱制御情報、および価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ３の秘密鍵Ｋｓｓｐで暗号化したデータである。

【００９４】

図２３は、図２１の例の場合における、取扱方針、取扱制御情報、価格情報、及び使用許諾条件の構成を示す図である。図２３に示す例の場合、コンテンツプロバイダ２の取扱方針（図２３（Ａ））は、そのまま価格情報を付しても、取扱方針と対比して価格情報を参照できる形式を有しない。そこで、サービスプロバイダ３は、その取扱方針を基に、価格情報と対比して価格情報を参照できる形式を有する取扱制御情報を生成し、それに価格情報を付して、ユーザホームネットワーク５に送信する（図２３（Ｂ））。ユーザホームネットワークでは、送信を受けた情報から使用許諾条件情報（図２３（Ｃ））を生成する。図２３のコンテンツプロバイダ２は、図１２の場合に比較し、より小さいデータ量の取扱方針を記録すればよい利点がある。

【００９５】

図２４は、EMDサービスセンタ１、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５の間で送受信されるコンテンツおよびコンテンツに付随する情報のさらに他の構成を説明する図である。図２１に示した例に対して、図２４の例では、取扱方針、取扱制御情報、価格情報、および課金情報は、共通鍵暗号により暗号化され、送信される。図２４のシステムは、

図２１の例の場合に比較して、システムの外部からの攻撃に対し、安全性が向上する。

【００９６】

図２５は、図２４の例の場合のコンテンツプロバイダセキュアコンテナを説明する図である。コンテンツプロバイダセキュアコンテナは、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、配送用鍵Ｋｄで暗号化された取扱方針、および署名を含む。署名は、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、および配送用鍵Ｋｄで暗号化された取扱方針にハッシュ関数を適用して生成されたハッシュ値を、コンテンツプロバイダ２の秘密鍵Ｋｓｃｐで暗号化したデータである。

【００９７】

図２６は、図２４の例の場合のサービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、配送用鍵Ｋｄで暗号化された取扱方針、コンテンツプロバイダ２により生成された署名、配送用鍵Ｋｄで暗号化された取扱制御情報、配送用鍵Ｋｄで暗号化された価格情報、および署名を含む。署名は、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、配送用鍵Ｋｄで暗号化された取扱方針、コンテンツプロバイダ２により生成された署名、配送用鍵Ｋｄで暗号化された取扱制御情報、および配送用鍵Ｋｄで暗号化された価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ３の秘密鍵Ｋｓｓｐで暗号化したデータである。

【００９８】

図２７は、EMDサービスセンタ１が、ユーザホームネットワーク５から課金情報を受信するときの動作を説明する図である。EMDサービスセンタ１と相互認証した後、レシーバ５１は、一時鍵Ｋｔｅｍｐを共有化し、共有化した一時鍵Ｋｔｅｍｐを用いて課金情報、および取扱方針等を暗号化し、EMDサービスセンタ１に送信する。ユーザ管理部１８はこれを受信する。ユーザ管理部１８は、受信し

た課金情報、および取扱方針等を共有化した一時鍵Ｋｔｅｍｐで復号化した後、経歴データ管理部１５および課金請求部１９に送信する。経歴データ管理部１５は決済を実行すると判定した場合、受信した課金情報を利益分配部１６に送信し、さらに、受信した課金情報および取扱方針等を課金請求部１９に送信する。利益分配部１６は、コンテンツプロバイダ２、サービスプロバイダ３、およびEMDサービスセンタ１自身に対する請求金額および支払金額を算出する。課金請求部１９は、ユーザの支払い金額を算出し、その情報を出納部２０に送信する。出納部２０は、図示せぬ外部の銀行等と通信し、決算処理を実行する。その際、ユーザの料金の未払い等の情報があれば、それらの情報は、課金請求部１９およびユーザ管理部１８に送信され、以後のユーザの登録処理時、または配送用鍵Ｋｄの送信処理時に参照される。ユーザ管理部１８はまた、鍵サーバ１４からの配送用鍵Ｋｄを一時鍵Ｋｔｅｍｐで暗号化しユーザホームネットワーク５に送信する。ユーザホームネットワーク５は、受信した配送用鍵Ｋｄを共有化した一時鍵Ｋｔｅｍｐで復号した後、配送用鍵Ｋｄを必要に応じて更新する。

【００９９】

図２８は、EMDサービスセンタ１の利益分配処理の動作を説明する図である。経歴データ管理部１５は、ユーザのコンテンツの使用実績を示す課金情報、取扱方針、および価格データを利益分配部１６に送信する。利益分配部１６は、これらの情報を基に、コンテンツプロバイダ２、サービスプロバイダ３、およびEMDサービスセンタ１それぞれの利益を算出し、その結果をサービスプロバイダ管理部１１、コンテンツプロバイダ管理部１２、出納部２０、および著作権管理部１３に送信する。出納部２０は、図示せぬ外部の銀行等と通信し、決算処理を実行する。サービスプロバイダ管理部１１は、サービスプロバイダ３の利益の情報をサービスプロバイダ３に送信する。コンテンツプロバイダ管理部１２は、コンテンツプロバイダ２の利益の情報をコンテンツプロバイダ２に送信する。監査部２１は、ユーザホームネットワーク５の機器から供給された課金情報、価格情報、および取扱方針の正当性を監査する。

【０１００】

図２９は、EMDサービスセンタ１の、コンテンツの利用実績の情報をJASRACに

送信する処理の動作を説明する図である。経歴データ管理部１５は、ユーザのコンテンツの使用実績を示す課金情報を著作権管理部１３および利益分配部１６に送信する。利益分配部１６は、JASRACに対する請求金額および支払金額を算出し、その情報を出納部２０に送信する。出納部２０は、図示せぬ外部の銀行等と通信し、決算処理を実行する。著作権管理部１３は、ユーザのコンテンツの使用実績をJASRACに送信する。

【０１０１】

次に、EMDシステムの処理について説明する。図３０は、このシステムのコンテンツの配布および再生の処理を説明するフローチャートである。ステップＳ１１において、EMDサービスセンタ１のコンテンツプロバイダ管理部１２は、コンテンツプロバイダ２に配送用鍵Ｋｄを送信し、コンテンツプロバイダ２がこれを受信する。その処理の詳細は、図３２のフローチャートを参照して後述する。ステップＳ１２において、ユーザは、ユーザホームネットワーク５の機器（例えば、図１０のレシーバ５１）を操作し、ユーザホームネットワーク５の機器をEMDサービスセンタ１のユーザ管理部１８に登録する。この登録処理の詳細は、図３６のフローチャートを参照して後述する。ステップＳ１３において、EMDサービスセンタ１のユーザ管理部１８は、ユーザホームネットワーク５と、図３３乃至図３５に示したように相互認証した後、ユーザホームネットワーク５の機器に、配送用鍵Ｋｄを送信する。ユーザホームネットワーク５はこの鍵を受信する。この処理の詳細は、図４５のフローチャートを参照して説明する。

【０１０２】

ステップＳ１４において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、サービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する。この送信処理の詳細は、図４７のフローチャートを参照して後述する。

【０１０３】

~~ステップＳ１５において、サービスプロバイダ３のセキュアコンテナ作成部４~~４は、ユーザホームネットワーク５からの要求に応じて、ネットワーク４を介して、ユーザホームネットワーク５にサービスプロバイダセキュアコンテナを送信する。この送信処理の詳細は、図４９のフローチャートを参照して後述する。な

お、ネットワーク４が、衛星通信により構成されている場合、サービスプロバイダセキュアコンテナの要求は、ユーザホームネットワーク５からサービスプロバイダ３に対して行われない。

【０１０４】

ステップＳ１６において、ユーザホームネットワーク５の課金モジュール７２は、課金処理を実行する。課金処理の詳細は、図５１のフローチャートを参照して後述する。ステップＳ１７において、ユーザは、ユーザホームネットワーク５の機器でコンテンツを再生する。再生処理の詳細は、図５２のフローチャートを参照して後述する。

【０１０５】

一方、コンテンツプロバイダ２が、取扱方針を暗号化して送信する場合の処理は、図３１のフローチャートで示すようになる。ステップＳ２１において、EMDサービスセンタ１のコンテンツプロバイダ管理部１２は、コンテンツプロバイダ２に配送用鍵Ｋｄを送信する。ステップＳ２２において、EMDサービスセンタ１のサービスプロバイダ管理部１１は、サービスプロバイダ３に配送用鍵Ｋｄを送信する。それ以降のステップＳ２３乃至ステップＳ２８の処理は、図３０のステップＳ１２乃至ステップＳ１７の処理と同様の処理であり、その説明は省略する。

【０１０６】

図３２は、図３０のステップＳ１１および図３１のステップＳ２１に対応する、EMDサービスセンタ１がコンテンツプロバイダ２へ配送用鍵Ｋｄを送信し、コンテンツプロバイダ２がこれを受信する処理の詳細を説明するフローチャートである。ステップＳ３１において、EMDサービスセンタ１の相互認証部１７は、コンテンツプロバイダ２の相互認証部３９と相互認証する。この相互認証処理の詳細は、図３３を参照して後述する。相互認証処理により、コンテンツプロバイダ２が、正当なプロバイダであることが確認されたとき、ステップＳ３２において、コンテンツプロバイダ２の暗号化部３４および暗号化部３６は、EMDサービスセンタ１のコンテンツプロバイダ管理部１２から送信された配送用鍵Ｋｄを受信する。ステップＳ３３において、コンテンツプロバイダ２の暗号化部３６は、受

信した配送用鍵Ｋｄを記憶する。

【０１０７】

このように、コンテンツプロバイダ２は、EMDサービスセンタ１から配送用鍵Ｋｄを受け取る。同様に、図３１に示すフローチャートの処理を行う例の場合、コンテンツプロバイダ２以外に、サービスプロバイダ３も、図３２と同様の処理で、EMDサービスセンタ１から配送用鍵Ｋｄを受け取る。

【０１０８】

次に、図３２のステップＳ３１における、いわゆるなりすましがないことを確認する相互認証の処理について、１つの共通鍵を用いる（図３３）、２つの共通鍵を用いる（図３４）、および公開鍵暗号を用いる（図３５）を例として説明する。

【０１０９】

図３３は、１つの共通鍵で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ２の相互認証部３９とEMDサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ４１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する（乱数生成部３５が生成するようにしてもよい）。ステップＳ４２において、コンテンツプロバイダ２の相互認証部３９は、DESを用いて乱数Ｒ１を、予め記憶している共通鍵Kcで暗号化する（暗号化部３６で暗号化するようにしてもよい）。ステップＳ４３において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ１をEMDサービスセンタ１の相互認証部１７に送信する。

【０１１０】

ステップＳ４４において、EMDサービスセンタ１の相互認証部１７は、受信した乱数Ｒ１を予め記憶している共通鍵Kcで復号する。ステップＳ４５において、EMDサービスセンタ１の相互認証部１７は、３２ビットの乱数Ｒ２を生成する。ステップＳ４６において、EMDサービスセンタ１の相互認証部１７は、復号した６４ビットの乱数Ｒ１の下位３２ビットを乱数Ｒ２で入れ替え、連接Ｒ１Ｈ‖Ｒ２を生成する。なお、ここでＲｉＨは、Ｒｉの上位ビットを表し、Ａ‖Ｂは、ＡとＢの連接（ｎビットのＡの下位に、ｍビットのＢを結合して、（ｎ＋ｍ）ビ

ットとしたもの）を表す。ステップＳ４７において、EMDサービスセンタ１の相互認証部１７は、DESを用いてＲ１Ｈ‖Ｒ２を共通鍵Ｋcで暗号化する。ステップＳ４８において、EMDサービスセンタ１の相互認証部１７は、暗号化したＲ１Ｈ‖Ｒ２をコンテンツプロバイダ２に送信する。

【０１１１】

ステップＳ４９において、コンテンツプロバイダ２の相互認証部３９は、受信したＲ１Ｈ‖Ｒ２を共通鍵Ｋcで復号する。ステップＳ５０において、コンテンツプロバイダ２の相互認証部３９は、復号したＲ１Ｈ‖Ｒ２の上位３２ビットＲ１Ｈを調べ、ステップＳ４１で生成した、乱数Ｒ１の上位３２ビットＲ１Ｈと一致すれば、EMDサービスセンタ１が正当なセンタであることを認証する。生成した乱数Ｒ１Ｈと、受信したＲ１Ｈが一致しないとき、処理は終了される。両者が一致するとき、ステップＳ５１において、コンテンツプロバイダ２の相互認証部３９は、３２ビットの乱数Ｒ３を生成する。ステップＳ５２において、コンテンツプロバイダ２の相互認証部３９は、受信し、復号した３２ビットの乱数Ｒ２を上位に設定し、生成した乱数Ｒ３をその下位に設定し、連接Ｒ２‖Ｒ３とする。ステップＳ５３において、コンテンツプロバイダ２の相互認証部３９は、DESを用いて連接Ｒ２‖Ｒ３を共通鍵Ｋcで暗号化する。ステップＳ５４において、コンテンツプロバイダ２の相互認証部３９は、暗号化された連接Ｒ２‖Ｒ３をEMDサービスセンタ１の相互認証部１７に送信する。

【０１１２】

ステップＳ５５において、EMDサービスセンタ１の相互認証部１７は、受信した連接Ｒ２‖Ｒ３を共通鍵Ｋcで復号する。ステップＳ５６において、EMDサービスセンタ１の相互認証部１７は、復号した連接Ｒ２‖Ｒ３の上位３２ビットを調べ、乱数Ｒ２と一致すれば、コンテンツプロバイダ２を正当なプロバイダとして認証し、一致しなければ、不正なプロバイダとして、処理を終了する。

【０１１３】

図３４は、２つの共通鍵Ｋｃ１，Ｋｃ２で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ２の相互認証部３９とEMDサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ６１にお

いて、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する。ステップＳ６２において、コンテンツプロバイダ２の相互認証部３９は、DESを用いて乱数Ｒ１を予め記憶している共通鍵Ｋｃ１で暗号化する。ステップＳ６３において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ１をEMDサービスセンタ１に送信する。

【０１１４】

ステップＳ６４において、EMDサービスセンタ１の相互認証部１７は、受信した乱数Ｒ１を予め記憶している共通鍵Ｋｃ１で復号する。ステップＳ６５において、EMDサービスセンタ１の相互認証部１７は、乱数Ｒ１を予め記憶している共通鍵Ｋｃ２で暗号化する。ステップＳ６６において、EMDサービスセンタ１の相互認証部１７は、６４ビットの乱数Ｒ２を生成する。ステップＳ６７において、EMDサービスセンタ１の相互認証部１７は、乱数Ｒ２を共通鍵Ｋｃ２で暗号化する。ステップＳ６８において、EMDサービスセンタ１の相互認証部１７は、暗号化された乱数Ｒ１および乱数Ｒ２をコンテンツプロバイダ２の相互認証部３９に送信する。

【０１１５】

ステップＳ６９において、コンテンツプロバイダ２の相互認証部３９は、受信した乱数Ｒ１および乱数Ｒ２を予め記憶している共通鍵Ｋｃ２で復号する。ステップＳ７０において、コンテンツプロバイダ２の相互認証部３９は、復号した乱数Ｒ１を調べ、ステップＳ６１で生成した乱数Ｒ１（暗号化する前の乱数Ｒ１）と一致すれば、EMDサービスセンタ１を適正なセンタとして認証し、一致しなければ、不正なセンタであるとして、処理を終了する。ステップＳ７１において、コンテンツプロバイダ２の相互認証部３９は、復号して得た乱数Ｒ２を共通鍵Ｋｃ１で暗号化する。ステップＳ７２において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ２をEMDサービスセンタ１に送信する。

【０１１６】

ステップＳ７３において、EMDサービスセンタ１の相互認証部１７は、受信した乱数Ｒ２を共通鍵Ｋｃ１で復号する。ステップＳ７４において、EMDサービスセンタ１の相互認証部１７は、復号した乱数Ｒ２が、ステップＳ６６で生成した

乱数Ｒ２（暗号化する前の乱数Ｒ２）と一致すれば、コンテンツプロバイダ２を適正なプロバイダとして認証し、一致しなければ、不正なプロバイダであるとして処理を終了する。

【０１１７】

図３５は、公開鍵暗号である、１６０ビット長の楕円曲線暗号を用いる、コンテンツプロバイダ２の相互認証部３９とEMDサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ８１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する。ステップＳ８２において、コンテンツプロバイダ２の相互認証部３９は、自分自身の公開鍵Ｋｐｃｐを含む証明書（認証局から予め取得しておいたもの）と、乱数Ｒ１をEMDサービスセンタ１の相互認証部１７に送信する。

【０１１８】

ステップＳ８３において、EMDサービスセンタ１の相互認証部１７は、受信した証明書の署名（認証局の秘密鍵Ｋｓｃａで暗号化されている）を、予め取得しておいた認証局の公開鍵Ｋｐｃａで復号し、コンテンツプロバイダ２の公開鍵Ｋｐｃｐとコンテンツプロバイダ２の名前のハッシュ値を取り出すとともに、証明書に平文のまま格納されているコンテンツプロバイダ２の公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前を取り出す。証明書が認証局が発行した適正なものであれば、証明書の署名を復号することが可能であり、復号して得られた公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前のハッシュ値は、平文のまま証明書に格納されていたコンテンツプロバイダ２の公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵Ｋｐｃｐが改竄されたものでない適正なものであることが認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しないときには、適正な公開鍵でないか、適正なプロバイダでないことになる。この時処理は終了される。

【０１１９】

適正な認証結果が得られたとき、ステップＳ８４において、EMDサービスセンタ１の相互認証部１７は、６４ビットの乱数Ｒ２を生成する。ステップＳ８５に

おいて、EMDサービスセンタ１の相互認証部１７は、乱数Ｒ１および乱数Ｒ２の連接Ｒ１‖Ｒ２を生成する。ステップＳ８６において、EMDサービスセンタ１の相互認証部１７は、連接Ｒ１‖Ｒ２を自分自身の秘密鍵Ｋｓｅｓｃで暗号化する。ステップＳ８７において、EMDサービスセンタ１の相互認証部１７は、連接Ｒ１‖Ｒ２を、ステップＳ８３で取得したコンテンツプロバイダ２の公開鍵Ｋｐｃｐで暗号化する。ステップＳ８８において、EMDサービスセンタ１の相互認証部１７は、秘密鍵Ｋｓｅｓｃで暗号化された連接Ｒ１‖Ｒ２、公開鍵Ｋｐｃｐで暗号化された連接Ｒ１‖Ｒ２、および自分自身の公開鍵Ｋｐｅｓｃを含む証明書（認証局から予め取得しておいたもの）をコンテンツプロバイダ２の相互認証部３９に送信する。

【０１２０】

ステップＳ８９において、コンテンツプロバイダ２の相互認証部３９は、受信した証明書の署名を予め取得しておいた認証局の公開鍵Ｋｐｃａで復号し、正しければ証明書から公開鍵Ｋｐｅｓｃを取り出す。この場合の処理は、ステップＳ８３における場合と同様であるので、その説明は省略する。ステップＳ９０において、コンテンツプロバイダ２の相互認証部３９は、EMDサービスセンタ１の秘密鍵Ｋｓｅｓｃで暗号化されている連接Ｒ１‖Ｒ２を、ステップＳ８９で取得した公開鍵Ｋｐｅｓｃで復号する。ステップＳ９１において、コンテンツプロバイダ２の相互認証部３９は、自分自身の公開鍵Ｋｐｃｐで暗号化されている連接Ｒ１‖Ｒ２を、自分自身の秘密鍵Ｋｓｃｐで復号する。ステップＳ９２において、コンテンツプロバイダ２の相互認証部３９は、ステップＳ９０で復号された連接Ｒ１‖Ｒ２と、ステップＳ９１で復号された連接Ｒ１‖Ｒ２を比較し、一致すればEMDサービスセンタ１を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

【０１２１】

適正な認証結果が得られたとき、ステップＳ９３において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ３を生成する。ステップＳ９４において、コンテンツプロバイダ２の相互認証部３９は、ステップＳ９０で取得した乱数Ｒ２および生成した乱数Ｒ３の連接Ｒ２‖Ｒ３を生成する。ステップＳ

９５において、コンテンツプロバイダ２の相互認証部３９は、連接Ｒ２‖Ｒ３を、ステップＳ８９で取得した公開鍵Ｋｐｅｓｃで暗号化する。ステップＳ９６において、コンテンツプロバイダ２の相互認証部３９は、暗号化した連接Ｒ２‖Ｒ３をEMDサービスセンタ１の相互認証部１７に送信する。

【０１２２】

ステップＳ９７において、EMDサービスセンタ１の相互認証部１７は、暗号化された連接Ｒ２‖Ｒ３を自分自身の秘密鍵Ｋｓｅｓｃで復号する。ステップＳ９８において、EMDサービスセンタ１の相互認証部１７は、復号した乱数Ｒ２が、ステップＳ８４で生成した乱数Ｒ２（暗号化する前の乱数Ｒ２）と一致すれば、コンテンツプロバイダ２を適正なプロバイダとして認証し、一致しなければ、不適正なプロバイダとして、処理を終了する。

【０１２３】

以上のように、EMDサービスセンタ１の相互認証部１７とコンテンツプロバイダ２の相互認証部３９は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵Ｋｔｅｍｐとして利用される。

【０１２４】

図３６は、図３０のステップＳ１２および図３１のステップＳ２３に対応する、レシーバ５１がEMDサービスセンタ１のユーザ管理部１８に登録する処理を説明するフローチャートである。ステップＳ１０１において、レシーバ５１のSAM６２は、ICカードインターフェース６４の出力から、レシーバ５１にバックアップ用のICカード５５が装着されているか否かを判定し、バックアップ用のICカード５５が装着されていると判定された場合（例えば、レシーバ５１が新たなレシーバ５１に変更され、元のレシーバ５１のデータを、新たなレシーバ５１に引き継ぐために、元のレシーバ５１のデータをバックアップ用のICカード５５にバックアップさせている場合）、ステップＳ１０２に進み、ICカード５５に記憶されているバックアップデータの読み込み処理を実行する。この処理の詳細は、図４１のフローチャートを参照して後述する。勿論、この読み込み処理が実行されるためには、その前に、ICカード５５に、バックアップデータを記憶させる必要があるが、その処理は、図３９を参照して後述する。

【０１２５】

ステップＳ１０１において、バックアップ用のICカード５５が装着されていないと判定された場合、手続は、ステップＳ１０２をスキップし、ステップＳ１０３に進む。ステップＳ１０３において、SAM６２の相互認証モジュール７１は、EMDサービスセンタ１の相互認証部１７と相互認証し、SAM６２は、証明書をEMDサービスセンタ１のユーザ管理部１８に送信する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１０３で、SAM６２がEMDサービスセンタ１のユーザ管理部１８に送信する証明書は、図３７に示すデータを含む。SAM６２が送信する証明書は、図１４に示すコンテンツプロバイダ２の証明書とほぼ同様の構成を有するが、更に、他のSAMに従属するか否かを示すデータを含んでいる。ステップＳ１０４において、SAM６２は、通信部６１を介して、一時鍵Ｋｔｅｍｐで暗号化した、ユーザの銀行等の決済機関の情報等をEMDサービスセンタ１のユーザ管理部１８に送信する。

【０１２６】

ステップＳ１０５において、EMDサービスセンタ１のユーザ管理部１８は、受信したSAM６２のIDを基に、図７に示したユーザ登録データベースを検索する。ステップＳ１０６において、EMDサービスセンタ１のユーザ管理部１８は、受信したIDを有するSAM６２の登録が可能であるか否かを判定し、受信したIDを有するSAM６２の登録が可能であると判定された場合、ステップＳ１０７に進み、受信したIDを有するSAM６２が、新規登録であるか否かを判定する。ステップＳ１０７において、受信したIDを有するSAM６２が、新規登録ではないと判定された場合、手続は、ステップＳ１０８に進む。

【０１２７】

ステップＳ１０８において、EMDサービスセンタ１のユーザ管理部１８は、更新登録を実行し、受信したIDを基にユーザ登録データベースを検索し、登録リストを作成する。この登録リストは、例えば、図３８に示す構造を有し、機器のSAMのIDに対応して、EMDサービスセンタ１のユーザ管理部１８が登録を拒絶したか否かを示す登録拒絶フラグ、従属する機器である場合のコンテンツ鍵Ｋｃｏの利用条件を示すステータスフラグ、従属する機器であるか否かを示すコンディショ

ンフラグ、並びに登録拒絶フラグ、ステータスフラグ、およびコンディションフラグにハッシュ関数を適用して生成したハッシュ値をEMDサービスセンタ１の秘密鍵Ｋｓｅｓｃで暗号化した署名から構成される。

【０１２８】

機器のSAMのIDは、機器の固有の６４ビットからなるIDを示す（図３８では、１６進数で示す）。登録拒絶フラグの”１”は、EMDサービスセンタ１のユーザ管理部１８が対応するIDを有する機器を登録したことを示し、登録拒絶フラグの”０”は、EMDサービスセンタ１のユーザ管理部１８が対応するIDを有する機器の登録を拒絶したことを示す。

【０１２９】

ステータスフラグのMSB(Most Significant Bit)の”１”は、対応するIDを有する子の機器（例えばレコーダ５３）が従属した親の機器（例えばレシーバ５１）からコンテンツ鍵Ｋｃｏをもらえることを示し、ステータスフラグのMSBの”０”は、対応するIDを有する子の機器が従属した親の機器からコンテンツ鍵Ｋｃｏをもらえないことを示している。ステータスフラグの上位から２ビット目の”１”は、対応するIDを有する子の機器が従属した親の機器から、親の機器の保存用鍵Ｋｓａｖｅで暗号化されたコンテンツ鍵Ｋｃｏをもらえることを示す。ステータスフラグの上位から３ビット目の”１”は、対応するIDを有する子の機器が従属した親の機器から、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏをもらえることを示す。ステータスフラグのLSB(Least Significant Bit)の”１”は、従属した親の機器が配送用鍵Ｋｄで暗号化したコンテンツ鍵Ｋｃｏを購入し、対応するIDを有する子の機器に、一時鍵Ｋｔｅｍｐで暗号化してコンテンツ鍵Ｋｃｏを渡すことを示す。

【０１３０】

コンディションフラグの”０”は、対応するIDを有する機器がEMDサービスセンタ１のユーザ管理部１８と直接通信が出来る（すなわち、例えばレシーバ５１のような親の機器である）ことを示し、コンディションフラグの”１”は、対応するIDを有する機器がEMDサービスセンタ１のユーザ管理部１８と直接通信が出来ない（すなわち、例えばレコーダ５３のような子の機器である）ことを示す。

コンディションフラグが”０”のとき、ステータスフラグは常に”００００”に設定される。

【０１３１】

ステップＳ１０９において、EMDサービスセンタ１のユーザ管理部１８は、相互認証部１７から供給された一時鍵Ｋｔｅｍｐで暗号化した、鍵サーバ１４から供給された配送用鍵Ｋｄをレシーバ５１のSAM６２に送信する。ステップＳ１１０において、レシーバ５１のSAM６２は、受信した配送用鍵Ｋｄを一時鍵Ｋｔｅｍｐで復号し、記憶モジュール７３に記憶させる。

【０１３２】

ステップＳ１１１において、EMDサービスセンタ１のユーザ管理部１８は、一時鍵Ｋｔｅｍｐで暗号化した登録リストをレシーバ５１のSAM６２に送信する。ステップＳ１１２において、レシーバ５１のSAM６２は、受信した登録リストを一時鍵Ｋｔｅｍｐで復号し、記憶モジュール７３に記憶させ、処理は終了する。

【０１３３】

ステップＳ１０７において、受信したIDを有するSAM６２が、新規登録であると判定された場合、手続は、ステップＳ１１４に進み、EMDサービスセンタ１のユーザ管理部１８は、新規登録を実行し、登録リストを作成し、ステップＳ１０９に進む。

【０１３４】

ステップＳ１０６において、受信したIDを有するSAM６２の登録が不可であると判定された場合、ステップＳ１１３に進み、EMDサービスセンタ１のユーザ管理部１８は、登録拒絶の登録リストを作成し、ステップＳ１１１に進む。

【０１３５】

このように、レシーバ５１は、EMDサービスセンタ１に登録される。

【０１３６】

次に、今まで使用していたレシーバ５１の記憶モジュール７３に記憶された配送用鍵Ｋｄなどの所定のデータをICカード５５に記憶させる処理の詳細を、図３９のフローチャートを参照して説明する。ステップＳ１２１において、SAM６２の相互認証モジュール７１は、ICカード５５の相互認証モジュール８０と相互認

証する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１２２において、SAM６２の乱数発生ユニット９２は、バックアップ鍵Ｋｉｃとして用いられる乱数を生成する。ステップＳ１２３において、SAM６２の暗号化ユニット９３は、記憶モジュール７３に記憶されているSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDを、バックアップ鍵Ｋｉｃを用いて暗号化する。ステップＳ１２４において、SAM６２の暗号化ユニット９３は、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃでバックアップ鍵Ｋｉｃを暗号化する（SAM６２は、EMDサービスセンタ１との間の認証処理（図３５のステップＳ８９）において、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃを取得している）。ステップＳ１２５において、レシーバ５１のSAM６２は、ICカードインターフェース６４を介して、暗号化されたSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のID並びに暗号化されたバックアップ鍵ＫｉｃをICカード５５に送信し、記憶モジュール８１に記憶させる。

【０１３７】

以上のように、SAM６２の記憶モジュール７３に記憶されたSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDは、バックアップ鍵Ｋｉｃを用いて暗号化され、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃを用いて暗号化されたバックアップ鍵Ｋｉｃと共に、ICカード５５の記憶モジュール８１に記憶される。

【０１３８】

今まで使用していたレシーバ５１の記憶モジュール７３に記憶された配送用鍵Ｋｄなどの所定のデータをICカード５５に記憶させる他の処理の例の詳細を、図４０のフローチャートを参照して説明する。ステップＳ１３１において、SAM６２の相互認証モジュール７１は、ICカード５５の相互認証モジュール８０と相互認証する。ステップＳ１３２において、SAM６２の暗号化ユニット９３は、記憶モジュール７３に記憶されているSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDを、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃを用いて暗号化する。ステップＳ１３３において、レシーバ５１のSAM６２は、ICカードインターフェース６４を介して、暗号化されたSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDをICカード５５に送信し、記憶モジュール８１に記憶させる。

【０１３９】

図４０に示す処理により、図３９に示した場合より簡単な処理で、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃを用いて暗号化されたSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDは、ICカード５５の記憶モジュール８１に記憶される。

【０１４０】

このように、ICカード５５にバックアップされたデータは、図３６のステップＳ１０２の処理で、新しいレシーバ５１に読み込まれる。図４１は、図３９に示す処理でバックアップされたデータを読み出す場合の処理を説明するフローチャートである。ステップＳ１４１において、新しいレシーバ５１のSAM６２の相互認証モジュール７１は、ICカード５５の相互認証モジュール８０と相互認証する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。

【０１４１】

ステップＳ１４２において、SAM６２は、ICカードインタフェース６４を介して、記憶モジュール８１に記憶された、バックアップ鍵Ｋｉｃで暗号化されている古いレシーバ５１の記憶モジュール７３のデータ（SAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDを示すバックアップデータ）、およびEMDサービスセンタ１の公開鍵Ｋｐｅｓｃで暗号化されているバックアップ鍵Ｋｉｃを読み出す。ステップＳ１４３において、SAM６２の相互認証モジュール７１は、通信部６１を介して、EMDサービスセンタ１の相互認証部１７と相互認証する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１４４において、SAM６２は、通信部６１を介して、バックアップ鍵Ｋｉｃで暗号化されている記憶モジュール７３のデータ、およびEMDサービスセンタ１の公開鍵Ｋｐｅｓｃで暗号化されているバックアップ鍵Ｋｉｃを、EMDサービスセンタ１のユーザ管理部１８に送信する。

【０１４２】

ステップＳ１４５において、EMDサービスセンタ１のユーザ管理部１８は、受信したバックアップ鍵Ｋｉｃを自分自身の秘密鍵Ｋｓｅｓｃで復号する。ステッ

プＳ１４６において、EMDサービスセンタ１のユーザ管理部１８は、受信したバックアップデータを、バックアップ鍵Ｋｉｃで復号する。ステップＳ１４７において、EMDサービスセンタ１のユーザ管理部１８は、復号したバックアップデータを、相互認証部１７から供給された一時鍵Ｋｔｅｍｐで、再度、暗号化する。ステップＳ１４８において、EMDサービスセンタ１のユーザ管理部１８は、一時鍵Ｋｔｅｍｐで暗号化されたバックアップデータを、レシーバ５１の通信部６１に送信する。

【０１４３】

ステップＳ１４９において、レシーバ５１の通信部６１は、EMDサービスセンタ１のユーザ管理部１８から受信したデータを、SAM６２に送信し、SAM６２は、そのデータを復号した後、記憶モジュール７３に記憶させる。ステップＳ１５０において、EMDサービスセンタ１のユーザ管理部１８は、ICカード５５にデータを記憶させた古い装置のSAM６２のIDに対応するユーザ登録データベース（図７）のデータを登録不可に設定し、処理を終了する。

【０１４４】

このように、新しいレシーバ５１は、ICカード５５のバックアップデータを読み込む。

【０１４５】

また、図３６のステップＳ１０２は、図４２に示すフローチャートで説明される処理でもよい。ステップＳ１６１乃至ステップＳ１６３は、図４１のステップＳ１４１乃至ステップＳ１４３とそれぞれ同様であるので、その説明は省略する。ステップＳ１６４において、SAM６２は、通信部６１を介して、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃで暗号化されているバックアップ鍵Ｋｉｃを、EMDサービスセンタ１のユーザ管理部１８に送信する。

【０１４６】

ステップＳ１６５において、EMDサービスセンタ１のユーザ管理部１８は、受信したバックアップ鍵Ｋｉｃを自分自身の秘密鍵Ｋｓｅｓｃで復号する。ステップＳ１６６において、EMDサービスセンタ１のユーザ管理部１８は、復号したバックアップ鍵Ｋｉｃを、相互認証部１７から供給された一時鍵Ｋｔｅｍｐで、再

度、暗号化する。ステップＳ１６７において、EMDサービスセンタ１のユーザ管理部１８は、一時鍵Ｋｔｅｍｐで暗号化されたバックアップ鍵Ｋｉｃを、レシーバ５１の通信部６１に送信し、バックアップ鍵Ｋｉｃの復号のサービスに対するユーザへの課金の処理をする。

【０１４７】

ステップＳ１６８において、レシーバ５１の通信部６１は、EMDサービスセンタ１のユーザ管理部１８から受信した一時鍵Ｋｔｅｍｐで暗号化されたバックアップ鍵Ｋｉｃを、SAM６２に送信し、SAM６２は、一時鍵Ｋｔｅｍｐで暗号化されたバックアップ鍵Ｋｉｃを復号する。ステップＳ１６９において、SAM６２は、復号されたバックアップ鍵Ｋｉｃで、ステップＳ１６２においてICカード５５から読み出された古いレシーバ５１の記憶モジュール７３のデータ（SAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDを示すバックアップデータ）を復号し、記憶モジュール７３に記憶させる。ステップＳ１７０において、EMDサービスセンタ１のユーザ管理部１８は、ICカード５５にデータを記憶させた古い装置のSAM６２のIDに対応するユーザ登録データベース（図７）のデータを登録不可に設定し、処理を終了する。

【０１４８】

図４２に示した読み込みの処理は、図４１に示した処理に比較し、レシーバ５１とEMDサービスセンタ１の送受信されるデータの量が少なくでき、従って、通信時間を短くできる。図４１のステップＳ１４８において、図４２のステップＳ１６７と同様に、EMDサービスセンタ１は、課金の処理を行ってもよい。

【０１４９】

図４０に示す処理でバックアップされたデータを読み出す場合の処理を、図４３に示すフローチャートを用いて説明する。ステップＳ１８１において、新しいレシーバ５１のSAM６２の相互認証モジュール７１は、ICカード５５の相互認証モジュール８０と相互認証する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１８２において、SAM６２は、ICカードインタフェース６４を介して、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃで暗号化されている古いレシーバ５１の記憶モジュール７

３のデータ（SAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDを示すバックアップデータ）を読み出す。

【０１５０】

ステップＳ１８３において、SAM６２の相互認証モジュール７１は、通信部６１を介して、EMDサービスセンタ１の相互認証部１７と相互認証する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１８４において、SAM６２は、通信部６１を介して、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃで暗号化されている記憶モジュール７３のデータを、EMDサービスセンタ１のユーザ管理部１８に送信する。

【０１５１】

ステップＳ１８５において、EMDサービスセンタ１のユーザ管理部１８は、受信した記憶モジュール７３のデータを自分自身の秘密鍵Ｋｓｅｓｃで復号する。ステップＳ１８６において、EMDサービスセンタ１のユーザ管理部１８は、復号したバックアップデータを、相互認証部１７から供給された一時鍵Ｋｔｅｍｐで、再度、暗号化する。ステップＳ１８７において、EMDサービスセンタ１のユーザ管理部１８は、一時鍵Ｋｔｅｍｐで暗号化されたバックアップデータを、レシーバ５１の通信部６１に送信する。

【０１５２】

ステップＳ１８８において、レシーバ５１の通信部６１は、EMDサービスセンタ１のユーザ管理部１８から受信したデータを、SAM６２に送信し、SAM６２は、そのデータを復号した後、記憶モジュール７３に記憶させる。ステップＳ１８９において、EMDサービスセンタ１のユーザ管理部１８は、ICカード５５にデータを記憶させた古い装置のSAM６２のIDに対応するユーザ登録データベース（図７）のデータを登録不可に設定する。

【０１５３】

このように、図４０に示す処理を用いたバックアップの場合、図４３に示す処理により、新しいレシーバ５１は、ICカード５５のバックアップデータを読み込む。

【０１５４】

レシーバ５１は、自分自身を登録する場合（図３０のステップＳ１２に対応する処理を実行する場合）、図３６のフローチャートに示す処理を実行するが、レシーバ５１に従属するレコーダ５３をEMDサービスセンタ１に登録する場合、図４４のフローチャートに示す処理を実行する。ステップＳ２０１において、レシーバ５１のSAM６２は、記憶モジュール７３に記憶された登録リストに、レコーダ５３のIDを書き込む。ステップＳ２０２において、レシーバ５１の相互認証モジュール７１は、EMDサービスセンタ１の相互認証部１７と相互認証する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。

【０１５５】

ステップＳ２０３において、EMDサービスセンタ１のユーザ管理部１８は、レシーバ５１のID（図３７に示すSAM６２の証明書に含まれるSAM６２のID）を基に、ユーザ登録データベースを検索し、レシーバ５１が登録不可であるか否かを判定し、レシーバ５１が登録不可ではないと判定された場合、ステップＳ２０４に進み、レシーバ５１のSAM62は、記憶モジュール７３に記憶している配送用鍵Ｋｄのバージョン、課金情報（後述の図５１に示すフローチャートのステップＳ３５７の処理で記憶される）、および登録リスト、並びにHDD５２に記録された取扱方針を一時鍵Ｋｔｅｍｐで暗号化し、通信部６１を介して送信する。ステップＳ２０５において、EMDサービスセンタ１のユーザ管理部１８は、受信したデータを復号した後、課金情報を処理し、図３８を参照して説明した、レシーバ５１から受信した登録リストのレコーダ５３に関する登録拒絶フラグ、およびステータスフラグなどのデータの部分を更新し、レシーバ５１に対応するデータに応じた署名を付する。

【０１５６】

ステップＳ２０６において、EMDサービスセンタ１のユーザ管理部１８は、レシーバ５１が有する配送用鍵Ｋｄのバージョンが最新か否かを判定し、レシーバ５１が有する配送用鍵Ｋｄのバージョンが最新であると判定された場合、ステップＳ２０７に進み、一時鍵Ｋｔｅｍｐで暗号化した、更新した登録リスト、および課金情報受信メッセージを、レシーバ５１に送信し、レシーバ５１は、更新し

た登録リスト、および課金情報受信メッセージを受信し、復号した後、記憶する。ステップＳ２０８において、レシーバ５１は、記憶モジュール７３に記憶された課金情報を消去し、登録リストを、EMDサービスセンタ１のユーザ管理部１８からステップＳ２０７において受信したものに更新し、ステップＳ２１１に進む。

【０１５７】

ステップＳ２０６において、レシーバ５１が有する配送用鍵Ｋｄのバージョンが最新のものではないと判定された場合、ステップＳ２０９に進み、EMDサービスセンタ１のユーザ管理部１８は、一時鍵Ｋｔｅｍｐで暗号化した、最新バージョンの配送用鍵Ｋｄ、更新した登録リスト、および課金情報受信メッセージを、レシーバ５１に送信し、レシーバ５１は、最新バージョンの配送用鍵Ｋｄ、更新した登録リスト、および課金情報受信メッセージを受信し、復号した後、記憶する。ステップＳ２１０において、レシーバ５１は、記憶モジュール７３に記憶された課金情報を消去し、登録リストを、EMDサービスセンタ１のユーザ管理部１８からステップＳ２０９において受信したものに更新し、配送用鍵Ｋｄを最新バージョンのものに更新し、ステップＳ２１１に進む。

【０１５８】

ステップＳ２１１において、レシーバ５１のSAM６２は、更新した登録リストを参照し、レコーダ５３が登録不可か否かを判定し、レコーダ５３が登録不可でないと判定された場合、ステップＳ２１２に進み、レシーバ５１とレコーダ５３は相互認証し、一時鍵Ｋｔｅｍｐを共有する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ２１３において、レコーダ５３に、一時鍵Ｋｔｅｍｐで暗号化した、登録完了メッセージ、および配送用鍵Ｋｄを送信し、レコーダ５３は、登録完了メッセージ、および配送用鍵Ｋｄを受信し、復号する。ステップＳ２１４において、レコーダ５３は、配送用鍵Ｋｄを更新し、処理は終了する。

【０１５９】

ステップＳ２０３において、レシーバ５１が登録不可であると判定された場合、および、ステップＳ２１１において、レコーダ５３が登録不可であると判定さ

れた場合、処理は終了する。

【０１６０】

以上のように、レシーバ５１に従属するレコーダ５３は、レシーバ５１を介して、EMDサービスセンタ１に登録される。

【０１６１】

図４５は、図３０のステップＳ１３において、EMDサービスセンタ１がレシーバ５１に送信した配送用鍵Ｋｄを、レシーバ５１が受け取る処理の詳細を説明するフローチャートである。ステップＳ２２１において、レシーバ５１の相互認証モジュール７１は、EMDサービスセンタ１の相互認証部１７と相互認証する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ２２２において、レシーバ５１のSAM６２は、通信部６１を介して、EMDサービスセンタ１のユーザ管理部１８に証明書を送信し、EMDサービスセンタ１のユーザ管理部１８は、証明書を受信する。ステップＳ２２３乃至ステップＳ２３０は、図４４のステップＳ２０３乃至ステップＳ２１０と同様の処理であるのでその説明は省略する。

【０１６２】

このように、レシーバ５１は、EMDサービスセンタ１のユーザ管理部１８から配送用鍵Ｋｄを受け取り、レシーバ５１の課金情報をEMDサービスセンタ１のユーザ管理部１８に送信する。

【０１６３】

次に、レシーバ５１に従属するレコーダ５３の配送用鍵Ｋｄの受け取り処理（図３８に示すステータスフラグが、レコーダ５３の配送用鍵Ｋｄの受け取りを許可する値を有する場合）を、図４６に示すフローチャートを用いて説明する。ステップＳ２４１において、レシーバ５１の相互認証モジュール７１およびレコーダ５３の図示せぬ相互認証モジュールは、相互認証する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。

【０１６４】

ステップＳ２４２において、レシーバ５１は、レシーバ５１の記憶モジュール

７３に記憶する登録リストにレコーダ５３のデータが載っているか否かを判定し、レシーバ５１の記憶モジュール７３に記憶する登録リストにレコーダ５３のデータが載っていると判定された場合、ステップＳ２４３に進み、レシーバ５１の記憶モジュール７３に記憶する登録リストを基に、レコーダ５３が登録不可であるか否かを判定する。ステップＳ２４３において、レコーダ５３が登録不可ではないと判定された場合、ステップＳ２４４に進み、レコーダ５３のSAM６６は、レシーバ５１のSAM６２に、内蔵する記憶モジュールに記憶している配送用鍵Ｋｄ（後述する図４６のステップＳ２５５でレシーバ５１から受け取っている）のバージョンおよび課金情報（後述する図５１に対応する処理のステップＳ３５７に相当する処理で記憶している）を一時鍵Ｋｔｅｍｐで暗号化して、送信し、レシーバ５１のSAM６２は、配送用鍵Ｋｄのバージョンおよび課金情報を受信し、復号する。

【０１６５】

ステップＳ２４５において、レシーバ５１の相互認証モジュール７１は、通信部６１を介して、EMDサービスセンタ１の相互認証部１７と、相互認証する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ２４６において、EMDサービスセンタ１のユーザ管理部１８は、レシーバ５１のIDを基に、ユーザ登録データベースを検索し、レシーバ５１が登録不可であるか否かを判定し、レシーバ５１が登録不可ではないと判定された場合、ステップＳ２４７に進み、レシーバ５１のSAM62は、通信部６１を介して、EMDサービスセンタ１のユーザ管理部１８に、一時鍵Ｋｔｅｍｐで暗号化した、記憶モジュール７３に記憶している配送用鍵Ｋｄのバージョン、課金情報、および登録リスト、HDD５２に記録している取扱方針、並びにレコーダ５３の課金情報を送信する。ステップＳ２４８において、EMDサービスセンタ１のユーザ管理部１８は、受信したデータを復号した後、課金情報を処理し、図３８で説明した、レシーバ５１から受信した登録リストのレコーダ５３に関する登録拒絶フラグ、ステータスフラグなどのデータの部分を更新し、レシーバ５１に対応するデータに応じた署名を付する。

【０１６６】

ステップＳ２４９乃至ステップＳ２５４の処理は、図４４に示すステップＳ２０６乃至ステップＳ２１１とそれぞれ同様であるので、その説明は省略する。

【０１６７】

ステップＳ２５４において、レシーバ５１のSAM６２は、更新した登録リストを参照し、レコーダ５３が登録不可か否かを判定し、レコーダ５３が登録不可でないと判定された場合、ステップＳ２５５に進み、レコーダ５３に、一時鍵Ｋｔｅｍｐで暗号化した、課金情報受信メッセージ、および配送用鍵Ｋｄを送信し、レコーダ５３は、課金情報受信メッセージ、および配送用鍵Ｋｄを受信し、復号する。ステップＳ２５６において、レコーダ５３のSAM６６は、内蔵する記憶モジュールに記憶している、課金情報を消去し、配送用鍵Ｋｄを最新のバージョンに更新する。

【０１６８】

ステップＳ２４２において、レシーバ５１の記憶モジュール７３に記憶する登録リストにレコーダ５３のデータが載っていないと判定された場合、ステップＳ２５７に進み、図４４に示したレコーダ５３の登録処理を実行し、ステップＳ２４４に進む。

【０１６９】

ステップＳ２４３において、レコーダ５３が登録不可であると判定された場合、ステップＳ２４６において、レシーバ５１が登録不可であると判定された場合、および、ステップＳ２５４において、レコーダ５３が登録不可であると判定された場合、処理は終了する。

【０１７０】

以上のように、レシーバ５１に従属するレコーダ５３は、レシーバ５１を介して、配送用鍵Ｋｄを受け取る。

【０１７１】

次に、図３０のステップＳ１４に対応する、コンテンツプロバイダ２がサービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する処理を、図４７のフローチャートを用いて説明する。ステップＳ２７１において、コンテンツプロバイダ２のウォータマーク付加部３２は、コンテンツサーバ３１から読み

出したコンテンツに、コンテンツプロバイダ２を示す所定のウォータマークを挿入し、圧縮部３３に供給する。ステップＳ２７２において、コンテンツプロバイダ２の圧縮部３３は、ウォータマークが挿入されたコンテンツをATRAC2等の所定の方式で圧縮し、暗号化部３４に供給する。ステップＳ２７３において、乱数発生部３５は、コンテンツ鍵Ｋｃｏとして用いる乱数を発生させ、暗号化部３４に供給する。ステップＳ２７４において、コンテンツプロバイダ２の暗号化部３４は、DESなどの所定の方式で、コンテンツ鍵Ｋｃｏを使用して、ウォータマークが挿入され、圧縮されたコンテンツを暗号化する。

【０１７２】

ステップＳ２７５において、暗号化部３６は、DESなどの所定の方式で、図３０のステップＳ１１の処理により、EMDサービスセンタ１から供給されている配送用鍵Ｋｄでコンテンツ鍵Ｋｃｏを暗号化する。ステップＳ２７６において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、およびポリシー記憶部３７から供給された取扱方針にハッシュ関数を適用してハッシュ値を算出し、自分自身の秘密鍵Ｋｓｃｐで暗号化し、図１３に示すような署名を作成する。ステップＳ２７７において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、ポリシー記憶部３７から供給される取扱方針、およびステップＳ２７６で生成した署名を含んだ、図１３に示すようなコンテンツプロバイダセキュアコンテナを作成する。

【０１７３】

ステップＳ２７８において、コンテンツプロバイダ２の相互認証部３９は、サービスプロバイダ３の相互認証部４５と相互認証する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ２７９において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、サービスプロバイダ３に、コンテンツプロバイダセキュアコンテナに、予め認証局から発行してもらった証明書を付して送信し、処理を終了する。

【０１７４】

以上のように、コンテンツプロバイダ２は、サービスプロバイダ３に、コンテ

ンツプロバイダセキュアコンテナを送信する。

【０１７５】

コンテンツ鍵Ｋｃｏと共に取扱方針を配送用鍵Ｋｄで暗号化する例の場合の、コンテンツプロバイダ２がサービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する他の処理の詳細を、図４８のフローチャートを用いて説明する。ステップＳ２９１乃至ステップＳ２９４の処理は、図４７のステップＳ２７１乃至ステップＳ２７４の処理とそれぞれ同様であり、その説明は省略する。ステップＳ２９５において、コンテンツプロバイダ２の暗号化部３６は、図３１のステップＳ２１の処理により、EMDサービスセンタ１から供給されている配送用鍵Ｋｄを用いて、DESなどの所定の方式で、コンテンツ鍵Ｋｃｏおよびポリシー記憶部３７から供給される取扱方針を暗号化する。

【０１７６】

ステップＳ２９６において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、および暗号化された取扱方針にハッシュ関数を適用しハッシュ値を算出し、自分自身の秘密鍵Ｋｓｃｐで暗号化し、図２５に示すような署名を作成する。ステップＳ２９７において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、暗号化された取扱方針、および署名を含んだ、図２５に示すようなコンテンツプロバイダセキュアコンテナを作成する。ステップＳ２９８およびステップＳ２９９の処理は、図４７のステップＳ２７８およびステップＳ２７９の処理とそれぞれ同様であり、その説明は省略する。

【０１７７】

このように、コンテンツプロバイダ２は、サービスプロバイダ３に、暗号化された取扱方針を含むコンテンツプロバイダセキュアコンテナを送信する。

【０１７８】

次に、図３０のステップＳ１５に対応する、サービスプロバイダ３がレシーバ５１にサービスプロバイダセキュアコンテナを送信する処理の詳細を図４９のフローチャートを用いて説明する。ステップＳ３１１において、サービスプロバイ

ダ３の値付け部４２は、コンテンツプロバイダ２のセキュアコンテナ作成部３８から送信されたコンテンツプロバイダセキュアコンテナに付された証明書に含まれる署名を確認し、証明書の改竄がなければ、コンテンツプロバイダ２の公開鍵Ｋｐｃｐを取り出す。証明書の署名の確認は、図３５のステップＳ８３における処理と同様であるので、その説明は省略する。

【０１７９】

ステップＳ３１２において、サービスプロバイダ３の値付け部４２は、コンテンツプロバイダ２のセキュアコンテナ作成部３８から送信されたコンテンツプロバイダセキュアコンテナの署名をコンテンツプロバイダ２の公開鍵Ｋｐｃｐで復号し、得られたハッシュ値が、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、および取扱方針にハッシュ関数を適用し得られたハッシュ値と一致することを確認し、コンテンツプロバイダセキュアコンテナの改竄がないことを確認する。改竄が発見された場合は、処理を終了する。

【０１８０】

コンテンツプロバイダセキュアコンテナに改竄がない場合、ステップＳ３１３において、サービスプロバイダ３の値付け部４２は、コンテンツプロバイダセキュアコンテナから取扱方針を取り出す。ステップＳ３１４において、サービスプロバイダ３の値付け部４２は、取扱方針を基に、図１７で説明した価格情報を作成する。ステップＳ３１５において、サービスプロバイダ３のセキュアコンテナ作成部４４は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、価格情報、並びに暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、コンテンツプロバイダ２により生成された署名、および価格情報にハッシュ関数を適用して得られたハッシュ値を、自分自身の秘密鍵Ｋｓｓｐで暗号化し、得られた値を署名として図１５に示すようなサービスプロバイダセキュアコンテナを作成する。

【０１８１】

ステップＳ３１６において、サービスプロバイダ３の相互認証部４５は、レシーバ５１の相互認証モジュール７１と相互認証する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。

ステップＳ３１７において、サービスプロバイダ３のセキュアコンテナ作成部４４は、レシーバ５１の通信部６１に、証明書を付したサービスプロバイダセキュアコンテナを送信し、処理を終了する。

【０１８２】

このように、サービスプロバイダ３は、レシーバ５１にサービスプロバイダセキュアコンテナを送信する。

【０１８３】

コンテンツプロバイダ２において、取扱方針が配送用鍵Ｋｄで暗号化され、かつ、サービスプロバイダ３が取扱制御情報を作成する例の場合の、サービスプロバイダ３がレシーバ５１にサービスプロバイダセキュアコンテナを送信する処理の詳細を、図５０のフローチャートを用いて説明する。ステップＳ３３１およびステップＳ３３２の処理は、図４９のステップＳ３１１およびステップＳ３１２の処理とそれぞれ同様であるので、その説明は省略する。ステップＳ３３３において、サービスプロバイダ３の値付け部４２は、コンテンツプロバイダセキュアコンテナに含まれる暗号化された取扱方針を復号する。ステップＳ３３４において、サービスプロバイダ３の値付け部４２は、取扱方針を基に、図２３で説明した取扱制御情報を作成する。ステップＳ３３５乃至ステップＳ３３８の処理は、図４９のステップＳ３１４およびステップＳ３１７の処理とそれぞれ同様であるので、その説明は省略する。

【０１８４】

このように、サービスプロバイダ３は、レシーバ５１に暗号化された取扱方針を含むサービスプロバイダセキュアコンテナを送信する。

【０１８５】

図３０のステップＳ１６に対応する、適正なサービスプロバイダセキュアコンテナを受信した後の、レシーバ５１の課金処理の詳細を、図５１のフローチャートを用いて説明する。ステップＳ３５１において、レシーバ５１の復号／暗号化モジュール７４は、配送用鍵Ｋｄでコンテンツ鍵Ｋｃｏを復号できるか否かを判定し、配送用鍵Ｋｄでコンテンツ鍵Ｋｃｏを復号できないと判定された場合、ステップＳ３５２で、レシーバ５１は、図４５で説明した配送用鍵Ｋｄの受け取り

処理を実行し、ステップＳ３５３に進む。ステップＳ３５１において、配送用鍵Ｋｄでコンテンツ鍵Ｋｃｏを復号できると判定された場合、手続は、ステップＳ３５２をスキップし、ステップＳ３５３に進む。ステップＳ３５３において、レシーバ５１の復号ユニット９１は、図３０のステップＳ１３の処理により、記憶モジュール７３に記憶されている配送用鍵Ｋｄで、コンテンツ鍵Ｋｃｏを復号する。

【０１８６】

ステップＳ３５４において、レシーバ５１の課金処理モジュール７２は、サービスプロバイダセキュアコンテナに含まれる取扱方針および価格情報を取り出し、図１９および図２０で説明した課金情報および使用許諾条件情報を生成する。ステップＳ３５５において、レシーバ５１の課金処理モジュール７２は、記憶モジュール７３に記憶している課金情報およびステップＳ３５４で算出された課金情報から、現在の課金が課金の上限以上であるか否かを判定し、現在の課金が課金の上限以上であると判定された場合、ステップＳ３５６に進み、レシーバ５１は図４５で説明した配送用鍵Ｋｄの受け取り処理を実行し、新たな配送用鍵Ｋｄを受け取り、ステップＳ３５７に進む。ステップＳ３５５において、現在の課金が課金の上限未満であると判定された場合、ステップＳ３５６はスキップされ、ステップＳ３５７に進む。

【０１８７】

ステップＳ３５７において、レシーバ５１の課金処理モジュール７２は、記憶モジュール７３に課金情報を記憶させる。ステップＳ３５８において、レシーバ５１の課金処理モジュール７２は、ステップＳ３５４にて生成した使用許諾条件情報をHDD５２に記録する。ステップＳ３５９において、レシーバ５１のSAM６２は、HDD５２にサービスプロバイダセキュアコンテナから取り出した取扱方針を記録させる。

【０１８８】

ステップＳ３６０において、レシーバ５１の復号／暗号化モジュール７４は、使用許諾条件情報の全体にハッシュ関数を適用しハッシュ値を算出する。ステップＳ３６１において、レシーバ５１の記憶モジュール７３は、使用許諾条件情報

のハッシュ値を記憶する。

【０１８９】

ステップＳ３６２において、レシーバ５１の暗号化ユニット９３は、コンテンツ鍵Ｋｃｏを保存用鍵Ｋｓａｖｅで暗号化する。ステップＳ３６３において、レシーバ５１のSAM６２は、暗号化されたコンテンツ鍵Ｋｃｏを HDD５２に記憶させる。

【０１９０】

以上のように、レシーバ５１は、課金情報を記憶モジュール７３に記憶すると共に、コンテンツ鍵Ｋｃｏを配送用鍵Ｋｄで復号し、再度、コンテンツ鍵Ｋｃｏを保存用鍵Ｋｓａｖｅで暗号化し、HDD５２に記録させる。保存用鍵Ｋｓａｖｅは、記憶モジュール７３に記憶されている。

【０１９１】

レコーダ５３も、同様の処理で、課金情報をSAM６６内の記憶モジュールに記憶すると共に、コンテンツ鍵Ｋｃｏを配送用鍵Ｋｄで復号し、再度、コンテンツ鍵Ｋｃｏを保存用鍵Ｋｓａｖｅで暗号化し、HDD５２に記録させる。保存用鍵Ｋｓａｖｅは、SAM６６内の記憶モジュールに記憶されている。なお、レシーバ５１とレシーバ５３においてそれぞれ保持される保存用鍵Ｋｓａｖｅは、通常、違う鍵データとされている。

【０１９２】

図３０のステップＳ１７に対応するレシーバ５１がコンテンツを再生する処理の詳細を、図５２のフローチャートを用いて説明する。ステップＳ３８１において、レシーバ５１の復号／暗号化モジュール７４は、HDD５２から、図５１のステップＳ３５８で記憶した使用許諾条件情報およびステップＳ３６３で記憶した暗号化されたコンテンツ鍵Ｋｃｏを読み出す。ステップＳ３８２において、レシーバ５１の復号／暗号化モジュール７４は、使用許諾条件情報の全体にハッシュ関数を適用しハッシュ値を算出する。

【０１９３】

ステップＳ３８３において、レシーバ５１の復号／暗号化モジュール７４は、ステップＳ３８２において算出されたハッシュ値が、図５１のステップＳ３６０

で記憶モジュール７３に記憶されたハッシュ値と一致するか否かを判定し、ステップＳ３８２において算出されたハッシュ値が、記憶モジュール７３に記憶されたハッシュ値と一致すると判定された場合、ステップＳ３８４に進み、使用回数の値などの使用許諾条件情報に含まれる所定の情報を更新する。ステップＳ３８５において、レシーバ５１の復号／暗号化モジュール７４は、更新した使用許諾条件情報の全体にハッシュ関数を適用しハッシュ値を算出する。ステップＳ３８６において、レシーバ５１の記憶モジュール７３は、ステップＳ３８５で算出した使用許諾条件情報のハッシュ値を記憶する。ステップＳ３８７において、レシーバ５１の復号／暗号化モジュール７４は、HDD５２に更新した使用許諾条件情報を記録させる。

【０１９４】

ステップＳ３８８において、SAM６２の相互認証モジュール７１と伸張部６３の相互認証モジュール７５は、相互認証し、SAM６２および伸張部６３は、一時鍵Ｋｔｅｍｐを記憶する。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数Ｒ１、Ｒ２、Ｒ３、またはその組み合わせが、一時鍵Ｋｔｅｍｐとして用いられる。ステップＳ３８９において、復号／暗号化モジュール７４の復号ユニット９１は、図５１のステップＳ３６３にてHDD５２に記録されたコンテンツ鍵Ｋｃｏを、記憶モジュール７３に記憶された保存用鍵Ｋｓａｖｅで復号する。ステップＳ３９０において、復号／暗号化モジュール７４の暗号化ユニット９３は、復号されたコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで暗号化する。ステップＳ３９１において、SAM６２は、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵Ｋｃｏを伸張部６３に送信する。

【０１９５】

ステップＳ３９２において、伸張部６３の復号モジュール７６は、コンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号する。ステップＳ３９３において、SAM６２は、HDD５２に記録されたコンテンツを読み出し、伸張部６３に送信する。ステップＳ３９４において、伸張部６３の復号モジュール７７は、コンテンツをコンテンツ鍵Ｋｃｏで復号する。ステップＳ３９５において、伸張部６３の伸張モジ

ュール７８は、復号されたコンテンツをATRAC2などの所定の方式で伸張する。ステップＳ３９６において、伸張部６３のウォータマーク付加モジュール７９は、伸張されたコンテンツにレシーバ５１を特定する所定のウォータマークを挿入する。ステップＳ３９７において、レシーバ５１は、図示せぬスピーカなどに再生されたコンテンツを出力し、処理を終了する。

【０１９６】

ステップＳ３８３において、ステップＳ３８２において算出されたハッシュ値が、記憶モジュール７３に記憶されたハッシュ値と一致しないと判定された場合、ステップＳ３９８において、SAM６２は、図示せぬ表示装置にエラーメッセージを表示させる等の所定のエラー処理を実行し、処理は終了する。

【０１９７】

このように、レシーバ５１は、コンテンツを再生する。

【０１９８】

図５３は、図１１の構成を有するユーザホームネットワーク５において、レシーバ５１がデコーダ５６にコンテンツを再生させる処理を説明するフローチャートである。ステップＳ４１１乃至ステップＳ４１７の処理は、図５２のステップＳ３８１乃至ステップＳ３８７の処理とそれぞれ同様であるので、その説明は省略する。

【０１９９】

ステップＳ４１８において、SAM６２の相互認証モジュール７１とデコーダ５６の相互認証モジュール１０１は、相互認証し、一時鍵Ｋｔｅｍｐが共有される。この認証処理は、図３３乃至図３５を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数Ｒ１、Ｒ２、Ｒ３、またはその組み合わせが、一時鍵Ｋｔｅｍｐとして用いられる。ステップＳ４１９において、復号／暗号化モジュール７４の復号ユニット９１は、HDD５２に記録されたコンテンツ鍵Ｋｃｏを、記憶モジュール７３に記憶された保存用鍵Ｋｓａｖｅで復号する。ステップＳ４２０において、復号／暗号化モジュール７４の暗号化ユニット９３は、復号されたコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで暗号化する。ステップＳ４２１において、SAM６２は、一時鍵Ｋｔｅｍｐで暗号化され

たコンテンツ鍵Ｋｃｏをデコーダ５６に送信する。

【０２００】

ステップＳ４２２において、デコーダ５６の復号モジュール１０２は、コンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号する。ステップＳ４２３において、SAM６２は、HDD５２に記録されたコンテンツを読み出し、デコーダ５６に送信する。ステップＳ４２４において、デコーダ５６の復号モジュール１０３は、コンテンツをコンテンツ鍵Ｋｃｏで復号する。ステップＳ４２５において、デコーダ５６の伸張モジュール１０４は、復号されたコンテンツをATRAC2などの所定の方式で伸張する。ステップＳ４２６において、デコーダ５６のウォータマーク付加モジュール１０５は、伸張されたコンテンツにデコーダ５６を特定する所定のウォータマークを挿入する。ステップＳ４２７において、デコーダ５６は、図示せぬスピーカなどに再生されたコンテンツを出力し、処理を終了する。

【０２０１】

ステップＳ４２８の処理は、図５２のステップＳ３９８の処理と同様であるので、その説明は省略する。

【０２０２】

以上のように、ユーザホームネットワークが図１１に示す構成を有する場合、レシーバ５１が受信したコンテンツは、デコーダ５６で再生される。

【０２０３】

なお、コンテンツは、音楽データを例に説明したが、音楽データに限らず、動画像データ、静止画像データ、文書データ、またはプログラムデータでもよい。その際、圧縮は、コンテンツの種類に適した方式、例えば、画像であればMPEG(Moving Picture Experts Group)などが利用される。ウォーターマークも、コンテンツの種類に適した形式のウォーターマークが利用される。

【０２０４】

また、共通鍵暗号は、ブロック暗号であるDESを使用して説明したが、NTT（商標）が提案するFEAL、IDEA(International Data Encription Algorithm)、または１ビット乃至数ビット単位で暗号化するストリーム暗号などでもよい。

【０２０５】

さらに、コンテンツおよびコンテンツ鍵Ｋｃｏの暗号化は、共通鍵暗号方式を利用するとして説明したが、公開鍵暗号方式でもよい。

【０２０６】

図５４は、本発明を適用したEMDシステムの他の構成例を表している。なお、図中、図１および図１０における場合と対応する部分については、同一の符号を付してある。すなわち、この例においては、ユーザホームネットワーク５に代えて、ユーザホームネットワーク２００が設けられ、そのユーザホームネットワーク２００には、レコーダ５３に代えて、レシーバ２０１およびレシーバ２０２が、レシーバ５１に従属（接続）されている。

【０２０７】

レシーバ２０１は、レシーバ５１と同様の構成を有しており、レシーバ５１のSAM６２および記憶モジュール７３のそれぞれに対応するSAM２１０および記憶モジュール２１１等を有し、そしてHDD２０３に接続されている。レシーバ２０２も、レシーバ５１と同様の構成を有しており、SAM２２０および記憶モジュール２２１等を有している。レシーバ２０２は、レシーバ２０１にも接続（従属）する。ただし、レシーバ２０２は、HDDのような記録媒体には接続されていない。

【０２０８】

レシーバ５１は、図１０に示す構成を有するが、この例において、SAM６２の記憶モジュール７３には、図３８で示した登録リストに代えて、図５５に示すような登録リストが記憶されている。この登録リストは、表形式に情報が記憶されているリスト部、および登録リストを保持する機器についての所定の情報が記憶されている対象SAM情報部より構成されている。

【０２０９】

対象SAM情報部には、この登録リストを保有する機器のSAMID、この例の場合、レシーバ５１のSAM６２のIDが（「対象SAMID」の欄に）記憶されている。対象SAM情報部にはまた、この登録リストの有効期限が（「有効期限」の欄に）記憶され、登録リストのバージョン番号が（「バージョン番号」の欄に）記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ５１には、レシーバ２０１およびレシーバ２０２の２機の機器が接続されているので

、自分自身を含む合計値３が（「接続されている機器数」の欄に）記憶されている。

【０２１０】

リスト部は、「SAMID」、「ユーザID」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、「状態情報」、「登録条件署名」、および「登録リスト署名」の９個の項目から構成され、この例の場合、レシーバ５１の登録条件、レシーバ２０１の登録条件、およびレシーバ２０２の登録条件として、それぞれの項目に所定の情報が記憶されている。

【０２１１】

「SAMID」には、機器のSAMのIDが記憶される。この例の場合、レシーバ５１のSAM６２のID、レシーバ２０１のSAM２１０のID、およびレシーバ２０２のSAM２２０のIDが記憶されている。「ユーザID」には、対応する機器（レシーバ５１、レシーバ２０１、およびレシーバ２０２）のユーザのユーザIDが記憶される。

【０２１２】

「購入処理」には、対応する機器が、コンテンツを購入（具体的には、使用許諾条件やコンテンツ鍵Ｋｃｏを購入）するための処理を行うことができるか否かを示す情報（”可”または”不可”）が記憶される。この例の場合、レシーバ５１およびレシーバ２０１は、コンテンツを購入するための処理を行うことができるので、それぞれに対応する「購入処理」には、”可”が記憶されている。レシーバ２０２は、購入したコンテンツを記録する、例えば、HDDのような記録媒体に接続されていないので、コンテンツを購入する処理を行うことができず、そのため、レシーバ２０２に対応する「購入処理」には、”不可”が記憶されている。

【０２１３】

「課金処理」には、対応する機器が、EMDサービスセンタ１との間で、課金処理を行うことができるか否かを示す情報（”可”または”不可”）が記憶される。なお、課金処理が行えるか否かは、EMDサービスセンタ１において、機器をEMDシステム登録する際に決定される。この例の場合、レシーバ５１は、レシーバ５１課金処理を行うことがでる機器として登録されているので、対応する「課金処

理」には、”可”が記憶されている。一方、レシーバ２０１およびレシーバ２０２は、この例の場合、課金処理を行うことができない機器として登録されているので、レシーバ２０１およびレシーバ２０２のそれぞれに対応する「課金処理」には、”不可”が記憶されている。なお、レシーバ２０２においては、コンテンツの購入がなされないので、課金は計上されず、課金自体の必要がない。

【０２１４】

「課金機器」には、対応する機器において計上された課金に対する課金処理を行う機器のSAMのIDが記憶される。この例の場合、レシーバ５１（SAM６２）は、自分自身の課金に対する課金処理を行うことができるので、その対応する「課金機器」には、レシーバ５１のSAM６２のIDが記憶されている。レシーバ５１はまた、課金処理を行うことができないレシーバ２０１に代わり、レシーバ２０１により計上される課金に対する課金処理を行うので、レシーバ２０１に対応する「課金機器」には、レシーバ５１のSAM６２のIDが記憶されている。レシーバ２０２においては、上述したように、コンテンツが購入されず、課金も計上されないので、レシーバ２０２に対する課金処理は必要とされない。そのため、レシーバ２０２対応する「課金機器」には、課金処理を行う機器が存在しないことを示す情報（”なし”）が記憶されている。

【０２１５】

「コンテンツ供給機器」には、対応する機器が、コンテンツの供給をサービスプロバイダ３からではなく、接続される他の機器から受ける場合、コンテンツを供給することができる機器のSAMのIDが記憶される。この例の場合、レシーバ５１およびレシーバ２０１は、コンテンツの供給をサービスプロバイダ３から受けるので、それぞれに対応する「コンテンツ供給機器」には、コンテンツを供給する機器が存在しない旨を示す情報（”なし”）が記憶されている。レシーバ２０２は、ネットワーク４に接続されていないことから、コンテンツの供給をサービスプロバイダ３から受けることができず、レシーバ５１またはレシーバ２０１からコンテンツの供給を受ける。そのため、レシーバ２０２に対応する「コンテンツ供給機機」には、レシーバ５１のSAM６２のIDおよびレシーバ２０１のSAM２１０のIDが記憶されている。

【０２１６】

「状態情報」には、対応する機器の動作制限条件が記憶される。何ら制限されていない場合は、その旨を示す情報（”制限なし”）、一定の制限が課せられている場合は、その旨を示す情報（”制限あり”）、また動作が停止される場合には、その旨を示す情報（”停止”）が記憶される。例えば、課金処理が成功しなかった場合、その機器に対応する「状態情報」には、”制限あり”が設定される（詳細は後述する）。この例の場合、「状態情報」に”制限あり”が設定された機器においては、すでに購入されたコンテンツの再生（解読）処理は実行されるが、新たなコンテンツを購入するための処理は実行されなくなる。すなわち、一定の制限が機器に課せられる。また、コンテンツの不正複製などの違反行為が発覚した場合、「状態情報」には、”停止”が設定され、機器の動作が停止される。これにより、その機器はEMDシステムからのサービスを、一切受けうることができなくなる。

【０２１７】

この例の場合、レシーバ５１、レシーバ２０１、およびレシーバ２０２に対して、何ら制限が課せられていないものとし、それぞれに対応する「状態情報」には、”なし”が設定されている。

【０２１８】

「登録条件署名」には、上述したように、各機器（レシーバ５１、レシーバ２０１、およびレシーバ２０２）の登録条件として、それぞれ、「SAMID」、「購入処理」、「課金処理」、「課金代行機器」、「コンテンツ供給機器」、「状態情報」、および「公開鍵」に記憶されている情報に対するEMDサービスセンタ１による署名が記憶されている。

【０２１９】

「登録リスト署名」には、登録リストに設定されている全てのデータに対する、EMDサービスセンタ１の署名が記憶されている。

【０２２０】

図５６は、レシーバ２０１のSAM２１０の記憶モジュール２１１に記憶されている、レシーバ２０１の登録リストを表している。この登録リストの対象SAM情

報部には、レシーバ２０１のSAM２１０のID、その登録リストの有効期限、バージョン番号、接続されている機器の数（この例では、レシーバ２０１には、レシーバ５１およびレシーバ２０２の２機が接続され、自分自身を含めた合計数３）が記憶されている。リスト部には、図５５のレシーバ５１の登録リストのリスト部と同様の情報が記憶されている。

【０２２１】

図５７は、レシーバ２０２のSAM２２０の記憶モジュール２２１に記憶されている、レシーバ２０２の登録リストを表している。この登録リストの対象SAM情報部には、レシーバ２０２のSAM２２０のID、その登録リストの有効期限、バージョン番号、接続されている機器の数（この例では、レシーバ２０２には、レシーバ５１およびレシーバ２０１の２機が接続され、自分自身を含めた合計数３）が記憶されている。リスト部には、この例の場合、図５５および図５６の登録リストのリスト部に登録されているレシーバ５１、レシーバ２０１、およびレシーバ２０２の登録条件のうち、レシーバ２０２の登録条件のみが記憶されている。

【０２２２】

次に、図５５、図５６、および図５７に示したそれぞれの登録リストを、レシーバ５１の記憶モジュール７３、レシーバ２０１の記憶モジュール２１１、およびレシーバ２０２の記憶モジュール２２１に記憶させるための処理手順を、図５８のフローチャートを参照して説明する。

【０２２３】

ステップＳ５０１において、レシーバ５１の登録処理が実行される。ステップＳ５０１における登録処理の詳細は、図５９のフローチャートに示されている。

【０２２４】

ステップＳ６０１乃至Ｓ６０８においては、図３６のステップＳ１０１乃至Ｓ１０８における場合と同様の処理が実行されるので、その説明は省略するが、ステップＳ６０８において、EMDサービスセンタ１のユーザ管理部１８は、ユーザ登録データベースに基づいて、図６０に示すような登録リストを作成する。ここで作成された登録リストは、図５５に示した登録リストにおいて、レシーバ５１の登録条件のみが登録されているものに相当する。

【０２２５】

ステップＳ６０９乃至Ｓ６１４においては、図３６のステップＳ１０９乃至Ｓ１１４における場合と同様の処理が実行されているので、その詳細の説明は省略するが、ステップＳ６１２において、レシーバ５１のSAM６２は、ステップＳ６１１で、EMDサービスセンタ１から送信された登録リストを、一時鍵Ｋｔｅｍｐで復号し、記憶モジュール７３に記憶させる。このように、図６０に示した登録リストが、レシーバ５１の記憶モジュール７３に記憶されたとき、処理は終了し、図５８のステップＳ５０２に進む。

【０２２６】

ステップＳ５０２において、レシーバ２０１およびレシーバ２０２の登録処理が実行される。ステップＳ５０２における登録処理の詳細は、図６１のフローチャートに示されている。

【０２２７】

ステップＳ７０１において、レシーバ５１のSAM６２は、HDD５２に記憶されている登録リスト（図６０）に、図６２に示すように、レシーバ２０１のSAM２１０のIDおよびレシーバ２０２のSAM２２０のIDを「SAMID」に書き加え、そしてそれらに対応して、所定の情報を、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」の各項目に書き込む。

【０２２８】

この例の場合、レシーバ２０１のSAM２１０のIDが設定された「SAMID」に対応して、「購入処理」に”可”が、「課金処理」に”不可”が、「課金機器」にレシーバ５１のSAM６２のIDが、そして「コンテンツ供給機器」に”なし”が書き込まれる。またレシーバ２０２のSAM２２０のIDが設定された「SAMID」に対応して、「購入処理」に”不可”が、「課金処理」に”不可”が、「課金機器」に”なし”が、そして「コンテンツ供給機器」にレシーバ５１のSAM６２のIDおよびレシーバ２０１のSAM２１０のIDが書き込まれる。なお、ここで、「購入処理」、「課金処理」、「課金機器」、および「コンテンツ供給機器」のそれぞれに書き込まれる情報は、例えば、レシーバ２０１およびレシーバ２０２が、レシーバ５１に接続される際に設定された条件により決定される。

【０２２９】

次に、ステップＳ７０２において、レシーバ５１とEMDサービスセンタ１との相互認証が行われる。この相互認証は、図３３乃至図３５を参照して説明した場合と同様の処理であるので、その説明は省略する。

【０２３０】

ステップＳ７０３において、レシーバ５１のSAM６２は、HDD５２に記憶されている、課金情報に関連した取扱方針を一時鍵Ｋｔｅｍｐで暗号化し、ステップＳ７０１で新たな情報が書き加えられた登録リスト、記憶モジュール７３に記憶されている配送用鍵Ｋｄのバージョン、および課金情報とともに、EMDサービスセンタ１に送信する。

【０２３１】

ステップＳ７０４において、EMDサービスセンタ１のユーザ管理部１８は、ステップＳ７０３で、レシーバ５１から送信されてきた情報を受信し、復号する。その後、EMDサービスセンタ１のユーザ管理部１８が、登録リストの「状態情報」に”停止”を設定すべき不正行為がレシーバ２０１およびレシーバ２０２において存在するか否かを確認する。

【０２３２】

次に、ステップＳ７０５において、EMDサービスセンタ１のユーザ管理部１８は、ユーザ登録データベースと、ステップＳ７０４でのユーザ管理部１８による確認結果に基づいて、レシーバ２０１およびレシーバ２０２の登録条件を登録リストのリスト部に設定し、それに署名を付して、レシーバ５１の登録リスト（図５５）、を作成し、そのリスト部の情報を記憶する。

【０２３３】

次に、ステップＳ７０６において、EMDサービスセンタ１のユーザ管理部１８は、ステップＳ７０５で作成された登録リスト（レシーバ５１の登録リスト）を、一時鍵Ｋｔｅｍｐで暗号化して、レシーバ５１に送信する。

【０２３４】

ステップＳ７０７において、レシーバ５１のSAM６２は、ステップＳ７０６で、EMDサービスセンタ１から送信された登録リストを受信し、復号した後、記憶

モジュール７３に記憶させる。これにより、ステップＳ７０６で送信されてきたレシーバ５１の登録リスト（図５５）が、ステップＳ６１２（図５９）で記憶された図６０に示した登録リストに代えて、記憶モジュール７３に記憶される。これにより、処理は終了され、図５８のステップＳ５０３に進む。

【０２３５】

ステップ５０３において、レシーバ５１とレシーバ２０１の相互認証が行われるが、この相互認証処理は、図３３乃至図３５を参照して説明した場合と同様の処理であるので、その説明は省略する。

【０２３６】

次に、ステップＳ５０４において、レシーバ５１のSAM６２は、ステップＳ７０７で記憶モジュール７３に記憶された登録リストから、レシーバ２０１の登録リスト（図５６）を生成してレシーバ２０１に送信する。

【０２３７】

ステップＳ５０５において、レシーバ２０１のSAM２１０は、ステップＳ５０４でレシーバ５１から送信された登録リストを受信し、復号した後、記憶モジュール２１１に記憶させる。これにより、図５６に示した登録リストが、記憶モジュール２１１に記憶される。

【０２３８】

次に、ステップ５０６において、レシーバ５１とレシーバ２０２の相互認証が行われるが、この相互認証処理は、図３３乃至図３５を参照して説明した場合と同様の処理であるので、その説明は省略する。

【０２３９】

ステップＳ５０７において、レシーバ５１のSAM６２は、ステップＳ７０７で記憶モジュール７３に記憶された登録リストのうち、レシーバ２０２の登録リスト（レシーバ２０２の登録条件のみが記憶されている登録リスト（図５７））を、レシーバ２０２に送信する。

【０２４０】

次に、ステップＳ５０８において、レシーバ２０２のSAM２２０は、ステップＳ５０７でレシーバ５１から送信された登録リストを受信し、復号した後、記憶

モジュール２２１に記憶させる。これにより、図５７に示した登録リストが、記憶モジュール２２１に記憶される。その後、処理は終了される。

【０２４１】

以上のようにして、レシーバ５１、レシーバ２０１、およびレシーバ２０２は、それぞれの登録リストを取得し、それを保持する。

【０２４２】

次に、上述したように作成され、各レシーバに保持された登録リストの利用方法を、図５１のフローチャートで説明した課金処理に対応させて説明する。

【０２４３】

図５１のフローチャートで説明された課金処理において、ステップＳ３５５で、現在の課金の合計が、予め設定された上限額以上であると判定された場合、ステップＳ３５６に進み、配送用鍵Ｋｄの受け取り処理が実行される。この例の場合、図４５のフローチャートで説明された手順に代わり、図６３のフローチャートに示されている手順に従って処理が実行される。

【０２４４】

すなわち、ステップＳ８０１において、レシーバ５１とEMDサービスセンタ１との相互認証が行われる。この相互認証は、図３３乃至図３５を参照して説明した場合と同様の処理であるので、その説明は省略する。

【０２４５】

次に、ステップＳ８０２において、レシーバ５１のSAM６２は、必要に応じて、EMDサービスセンタ１のユーザ管理部１８に証明書を送信する。ステップＳ８０３において、レシーバ５１のSAM６２は、HDD５２に記憶されている、課金に関連する取扱方針を一時鍵Ｋｔｅｍｐで暗号化して、記憶モジュール７３に記憶されている配送用鍵Ｋｄのバージョン、課金情報、および登録リストとともに、EMDサービスセンタ１に送信する。

【０２４６】

ステップＳ８０４において、EMDサービスセンタ１のユーザ管理部１８は、ステップＳ８０３で、レシーバ５１から送信された情報を受信し、復号した後、EMDサービスセンタ１の監査部２１が、登録リストの「状態情報」に”停止”が設

出証特平１１－３０５９１５２

定されるべき不正行為がレシーバ５１、レシーバ２０１、およびレシーバ２０２において存在するか否かを確認する。

【０２４７】

次に、ステップＳ８０５において、EMDサービスセンタ１のユーザ管理部１８は、ステップＳ８０４での確認結果に基づいて、レシーバ５１に不正行為が存在するか否かを判定し、レシーバ５１に不正行為が存在しないと判定した場合、ステップＳ８０６に進む。

【０２４８】

ステップＳ８０６において、EMDサービスセンタ１の課金請求部１９は、ステップＳ８０３で受信された課金情報を解析し、ユーザの支払い金額を算出する処理等を行う。次に、ステップＳ８０７において、EMDサービスセンタ１のユーザ管理部１８は、ステップＳ８０６における処理により、決済が成功したか否かを確認し、その確認結果に基づいて、返却メッセージを作成する。この場合、レシーバ５１およびレシーバ２０１の両者の課金に対する決済が共に成功したとき（全ての機器に対する決済が成功したとき）、成功返却メッセージが作成される。また、レシーバ５１またはレシーバ２０１のいずれか一方の課金に対する決済が成功しなかったとき、またはレシーバ５１およびレシーバ２０１の両者の課金に対する決済が成功しなかったとき（全ての機器に対する決済が成功しなかったとき）、失敗返却メッセージが作成される。

【０２４９】

次に、ステップＳ８０８において、EMDサービスセンタ１のユーザ管理部１８は、ユーザ登録データベース、ステップＳ８０４における不正行為が存在するか否かの確認結果、およびステップＳ８０７における決済が成功したか否かの確認結果に基づいて、レシーバ５１、レシーバ２０１、およびレシーバ２０２の登録条件を設定し、それに署名を付して、登録リストをそれぞれ作成する。

【０２５０】

例えば、ステップＳ８０４で、レシーバ２０１またはレシーバ２０２において不正行為が確認された場合、それらに対応する「状態情報」には”停止”が設定され、この場合、今後、全ての処理が停止される。すなわち、EMDシステムから

のサービスを一切受けることができなくなる。また、ステップＳ８０７で、決済が成功しなかったと確認された場合、「状態情報」には”制限あり”が設定され、この場合、すでに購入したコンテンツを再生する処理は可能とされるが、新たにコンテンツを購入する処理は実行できなくなる。

【０２５１】

次に、ステップＳ８０９に進み、EMDサービスセンタ１のユーザ管理部１８は、一時鍵Ｋｔｅｍｐで、最新バージョンの配送用鍵Ｋｄ（図３で示した３月分の最新バージョンの配送用鍵Ｋｄ）およびステップＳ８０８で作成された登録リストを暗号化し、ステップＳ８０７で作成された返却メッセージとともにレシーバ５１に送信する。

【０２５２】

ステップＳ８１０において、レシーバ５１のSAM６２は、ステップＳ８０９でEMDサービスセンタ１から送信された情報を受信し、復号した後、記憶モジュール７３に記憶させる。このとき、記憶モジュール７３に記憶されていた課金情報は消去され、自分の登録リストおよび配送用鍵Ｋｄは更新される。

【０２５３】

次に、ステップＳ８１１において、レシーバ５１のSAM６２は、ステップＳ８１０で受信した返却メッセージが、成功返却メッセージであったかまたは失敗返却メッセージであったかを判定し、成功返却メッセージであったと判定した場合、ステップＳ８１２に進む。

【０２５４】

ステップＳ８１２において、レシーバ５１のSAM６２は、レシーバ２０１およびレシーバ２０２に対して、それぞれ相互認証処理（図３３乃至図３５を参照して説明した処理）を行った後、レシーバ２０１およびレシーバ２０２のそれぞれに、それぞれの登録リストと、配送用鍵Ｋｄを送信する。

【０２５５】

ステップＳ８１１において、ステップＳ８１０で受信した返却メッセージが、失敗返却メッセージであったと判定した場合、レシーバ５１のSAM６２は、ステップＳ８１３に進み、ステップＳ８０１で記憶モジュール７３に記憶させた登録

リスト（更新された登録リスト）を参照し、”制限あり”が「状態情報」に設定されているレシーバ（この例の場合、レシーバ５１の自分自身、またはレシーバ２０１）を検出する。

【０２５６】

次に、ステップＳ８１４において、レシーバ５１のSAM６２は、ステップＳ８１０で検出したレシーバに対して、所定の処理（REVOKE処理）を実行し、そのレシーバにおいて実行される処理を制限する。すなわち、この場合、新たにコンテンツを購入するための処理が実行できないようにする。

【０２５７】

ステップＳ８０５において、レシーバ５１において不正行為が確認された場合、ステップＳ８１５に進み、EMDサービスセンタ１は、レシーバ５１、レシーバ２０１、およびレシーバ２０２に対応する「状態情報」の全てに”停止”を設定し、登録リストを作成し、ステップＳ８１６において、レシーバ５１に送信する。なお、図３６のフローチャートで示した登録処理を、レシーバ２０１またはレシーバ２０２に対して行うことより、レシーバ２０１またはレシーバ２０２におけるコンテンツの利用が可能となる。

【０２５８】

次に、ステップＳ８１７において、レシーバ５１は、ステップＳ８１６でEMDサービスセンタ１から送信された登録リストを受信し、登録リストを更新する。すなわち、この場合、配送用鍵Ｋｄは、レシーバ５１、レシーバ２０１、およびレシーバ２０２には、供給されず、レシーバ５１、レシーバ２０１、およびレシーバ２０２は、供給されるコンテンツを再生することができなくなり、その結果、EMDシステムにおけるサービスを一切受けることができなくなる。

【０２５９】

ステップＳ８１２において、レシーバ２０１およびレシーバ２０２に登録リストおよび配送用鍵Ｋｄが送信されたとき、ステップＳ８１４において、「状態情報」に”制限あり”が設定されたレシーバに対してREVOKE処理が実行されたとき、またはステップＳ８１７において、「状態情報」に”停止”が設定された登録リストに更新されたとき、処理は終了され、図５１のステップＳ３５７に進む。

【０２６０】

ステップＳ３５７乃至Ｓ３６５における処理は、すでに説明されているので、ここでの説明は省略する。

【０２６１】

以上のように、登録リストがEMDサービスセンタ１に送信されると（図６３のステップＳ８０３）、EMDサービスセンタ１において、レシーバの不正行為が確認され、また処理（この例の場合、決済処理）が成功したか否かが確認され（ステップＳ８０７）、それらの確認結果に基づいて、登録リストが更新される。さらに、このようにして更新された登録リストは、各レシーバに保持されるようにしたので、各レシーバの動作を制御することができる。

【０２６２】

以上においては、ステップＳ３５５において、計上された課金が予め設定された上限額を超えた場合、ステップＳ３５６に進み、配送用鍵Ｋｄの受け取り処理が実行されるようにしたが、購入されるコンテンツの個数の上限数を設定し、購入されたコンテンツの個数がその上限数を超えた場合においても、ステップＳ３５６に進むようにすることもできる。

【０２６３】

また、以上においては、課金処理における場合を例として、登録リストの利用方法を説明したが、コンテンツが復号される場合、取扱方針に含まれるコンテンツ鍵Ｋｃｏのバージョンが、レシーバ５１のSAM６２で保持される配送用鍵Ｋｄのバージョンより新しいときなども、登録リストがレシーバ５１よりEMDサービスセンタ１に送信される。この場合においても、登録リストは、上述したように、EMDサービスセンタ１において作成され、各レシーバにおいて配布される。

【０２６４】

また、以上においては、機器（例えば、レシーバ５１、またはレシーバ２０１）が接続されるタイミングで、登録リストが課金情報とともにEMDサービスセンタ１に送信される場合を例として説明したが、このとき登録リストのみが送信されるようにすることもできる。また、以上においては、機器が登録されるときに課金情報が、EMDサービスセンタ１に送信される場合を例として説明したが、そ

れ以外のタイミングで課金情報をEMDサービスセンタ１に送信するようにしてもよい。

【０２６５】

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

【０２６６】

また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

【０２６７】

【発明の効果】

請求項１に記載の管理装置、請求項４に記載の管理方法、および請求項５に記載の提供媒体によれば、情報処理装置のIDおよびそのIDに対応して登録の可否を示すデータを有し、情報処理装置のIDを基に、情報処理装置を登録するようにしたので、迅速にユーザの契約の可否が判断できるようになる。

【０２６８】

請求項６に記載の情報処理装置、請求項８に記載の情報処理方法、および請求項９に記載の提供媒体によれば、情報処理装置に従属する他の情報処理装置の登録を請求するようにしたので、複数の情報処理装置を有するユーザも簡単に契約の処理ができるようになる。

【０２６９】

請求項１０に記載のシステムによれば、管理装置が、情報処理装置のIDおよびそのIDに対応して登録の可否を示すデータを有し、情報処理装置のIDを基に、情報処理装置を登録し、情報処理装置が、情報処理装置に従属する他の情報処理装置の登録を請求するようにしたので、迅速にユーザの契約の可否が判断でき、複数の情報処理装置を有するユーザも簡単に契約の処理ができるようになる。

【０２７０】

請求項１１に記載の情報処理装置、請求項１２に記載の情報処理方法、および請求項１３に記載の提供媒体によれば、登録条件を記憶するようにしたので、違

反などがあった場合の動作を簡単かつ確実に制御（制限）することができる。

【０２７１】

請求項１４に記載の管理装置、請求項１５に記載の管理方法、および請求項１６に記載の提供媒体によれば、所定の処理を実行するとき、登録条件を作成するようにしたので、違反などがあった場合の情報処理装置の動作を簡単にかつ確実に制御（制限）することができる。

【図面の簡単な説明】

【図１】

EMDのシステムを説明する図である。

【図２】

EMDサービスセンタ１の機能の構成を示すブロック図である。

【図３】

EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する図である。

【図４】

EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する図である。

【図５】

EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する図である。

【図６】

EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する図である。

【図７】

ユーザ登録データベースを説明する図である。

【図８】

コンテンツプロバイダ２の機能の構成を示すブロック図である。

【図９】

サービスプロバイダ３の機能の構成を示すブロック図である。

【図１０】

ユーザホームネットワーク５の構成を示すブロック図である。

【図１１】

ユーザホームネットワーク５の構成を示すブロック図である。

【図１２】

コンテンツおよびコンテンツに付随する情報を説明する図である。

【図１３】

コンテンツプロバイダセキュアコンテナを説明する図である。

【図１４】

コンテンツプロバイダ２の証明書を説明する図である。

【図１５】

サービスプロバイダセキュアコンテナを説明する図である。

【図１６】

サービスプロバイダ３の証明書を説明する図である。

【図１７】

取扱方針、価格情報、および使用許諾条件情報を示す図である。

【図１８】

シングルコピーおよびマルチコピーを説明する図である。

【図１９】

取扱方針および価格情報を説明する図である。

【図２０】

取扱方針、価格情報、および使用許諾条件情報を説明する図である。

【図２１】

コンテンツおよびコンテンツに付随する情報の他の構成を説明する図である。

【図２２】

サービスプロバイダセキュアコンテナを説明する図である。

【図２３】

取扱方針、取扱制御情報、価格情報、及び使用許諾条件の構成を示す図である

。

【図２４】

コンテンツおよびコンテンツに付随する情報の他の構成を説明する図である。

【図２５】

コンテンツプロバイダセキュアコンテナを説明する図である。

【図２６】

サービスプロバイダセキュアコンテナを説明する図である。

【図２７】

EMDサービスセンタ１の、ユーザホームネットワーク５からの課金情報の受信のときの動作を説明する図である。

【図２８】

EMDサービスセンタ１の利益分配処理の動作を説明する図である。

【図２９】

EMDサービスセンタ１の、コンテンツの利用実績の情報をJASRACに送信する処理の動作を説明する図である。

【図３０】

コンテンツの配布の処理を説明するフローチャートである。

【図３１】

コンテンツの配布の処理を説明するフローチャートである。

【図３２】

EMDサービスセンタ１がコンテンツプロバイダ２へ配送用鍵Ｋｄを送信する処理を説明するフローチャートである。

【図３３】

コンテンツプロバイダ２とEMDサービスセンタ１との相互認証の動作を説明するフローチャートである。

【図３４】

コンテンツプロバイダ２とEMDサービスセンタ１との相互認証の動作を説明するフローチャートである。

【図３５】

コンテンツプロバイダ２とEMDサービスセンタ１との相互認証の動作を説明するフローチャートである。

【図３６】

レシーバ５１のEMDサービスセンタ１への登録の処理を説明するフローチャートである。

【図３７】

SAMの証明書を説明する図である。

【図３８】

登録リストを説明する図である。

【図３９】

ICカード５５へのSAM６２のデータのバックアップの処理を説明するフローチャートである。

【図４０】

ICカード５５へのSAM６２のデータのバックアップの処理を説明するフローチャートである。

【図４１】

新しいレシーバにICカード５５のバックアップデータを読み込ませる処理を説明するフローチャートである。

【図４２】

新しいレシーバにICカード５５のバックアップデータを読み込ませる処理を説明するフローチャートである。

【図４３】

新しいレシーバにICカード５５のバックアップデータを読み込ませる処理を説明するフローチャートである。

【図４４】

レシーバ５１が、従属関係のあるレコーダ５３をEMDサービスセンタ１に登録する処理を説明するフローチャートである。

【図４５】

レシーバ５１がEMDサービスセンタ１から配送用鍵Ｋｄを受け取る処理を説明するフローチャートである。

【図４６】

レコーダの配送用鍵Ｋｄの受け取り処理を説明するフローチャートである。

【図４７】

コンテンツプロバイダ２がサービスプロバイダ３にコンテンツプロバイダセキ

ュアコンテナを送信する処理を説明するフローチャートである。

【図４８】

コンテンツプロバイダ２がサービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する他の処理を説明するフローチャートである。

【図４９】

サービスプロバイダ３がレシーバ５１にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図５０】

サービスプロバイダ３がレシーバ５１にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図５１】

レシーバ５１の課金処理を説明するフローチャートである。

【図５２】

レシーバ５１がコンテンツを再生する処理を説明するフローチャートである。

【図５３】

レシーバ５１がデコーダ５６にコンテンツを再生させる処理を説明するフローチャートである。

【図５４】

他のEMDシステムを説明する図である。

【図５５】

登録リストを説明する他の図である。

【図５６】

登録リストを説明する他の図である。

【図５７】

登録リストを説明する他の図である。

【図５８】

登録リストを保持するための処理を説明するフローチャートである。

【図５９】

レシーバ５１の登録処理を説明するフローチャートである。

【図６０】

登録リストを説明する他の図である。

【図６１】

レシーバ２０１およびレシーバ２０２の登録処理を説明するフローチャートである。

【図６２】

登録リストを説明する他の図である。

【図６３】

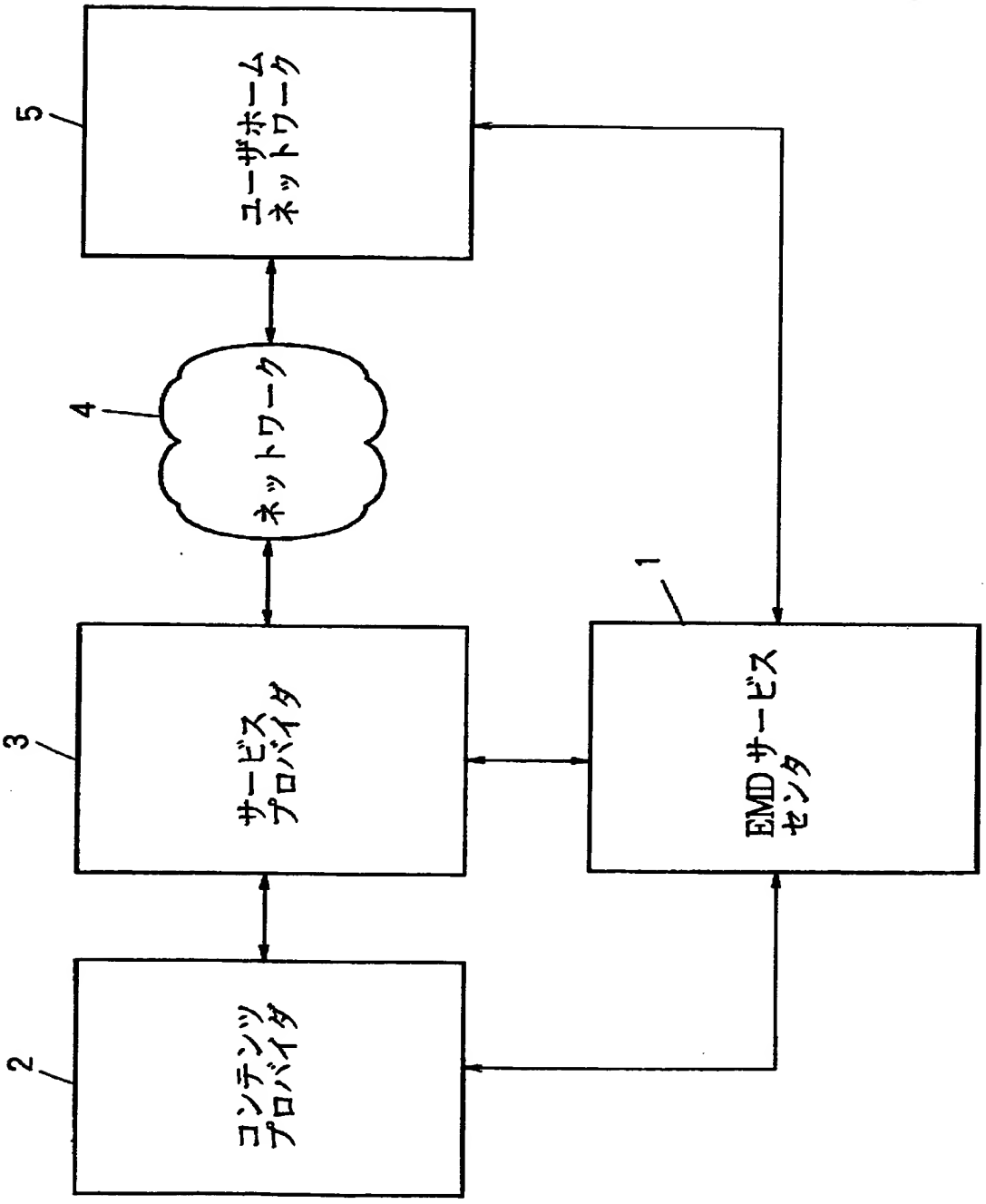
配送用鍵の受け取り処理を説明するフローチャートである。

【符号の説明】

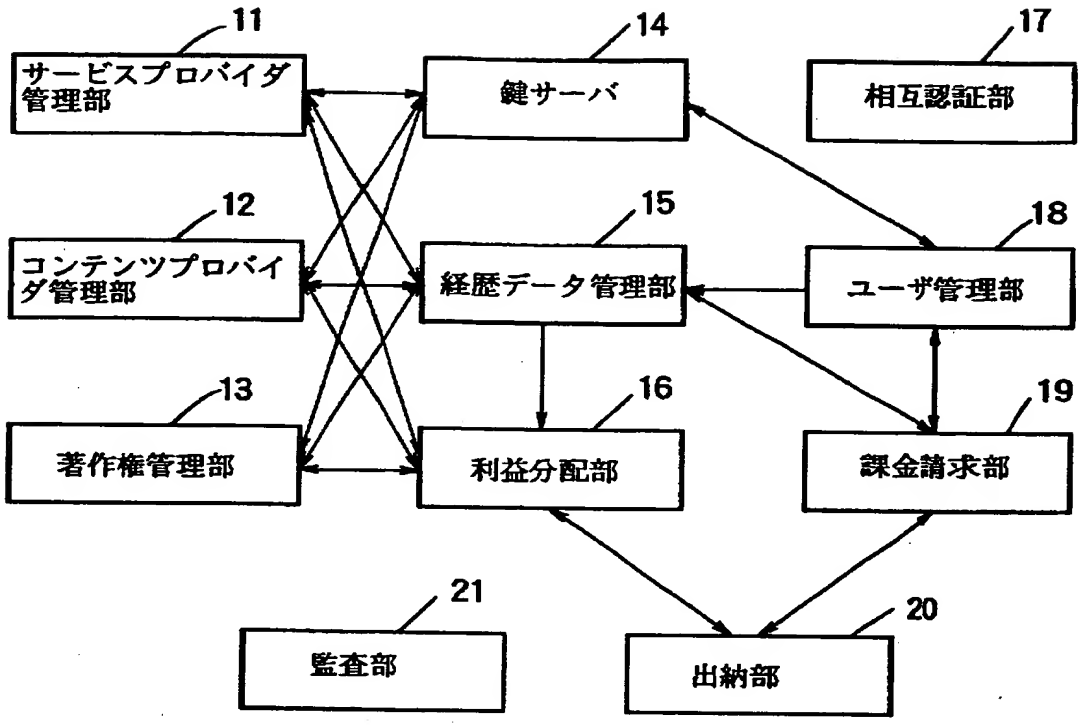
１　EMDサービスセンタ，　２　コンテンツプロバイダ、　３　サービスプロバイダ，５　ユーザホームネットワーク，　１６　利益分配部，　１８　ユーザ管理部，　４２　値付け部，　５１　レシーバ，　５６　デコーダ，　６１　通信部，　６２　SAM，　６３　伸張部，　７１　相互認証モジュール，　７２　課金処理モジュール，　７３　記憶モジュール，　７４　復号／暗号化モジュール，　７５　相互認証モジュール，　７６　復号モジュール，　７７　復号モジュール，　８０　相互認証モジュール，　８１　記憶モジュール，　９１　復号ユニット，　９２　乱数発生ユニット，　９３　暗号化ユニット，　１０１　相互認証モジュール，　１０２　復号モジュール，　１０３　復号モジュール，　２０１　レシーバ，　２０２　レシーバ，　２０３　HDD，　２１０　SAM，　２１１　記憶モジュール，　２２０　SAM，　２２１　記憶モジュール

【書類名】　図面

【図１】

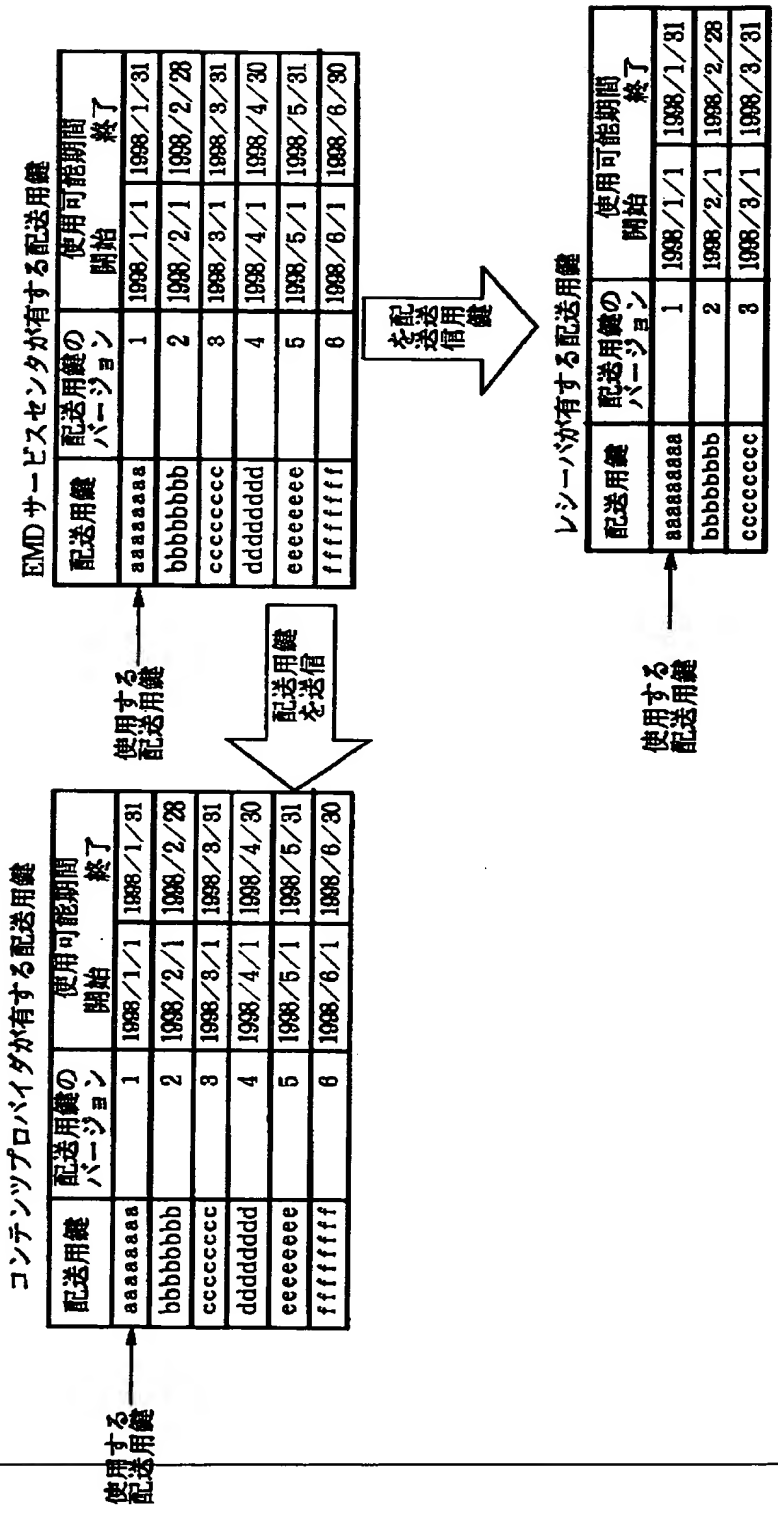

5
ユーザホーム
ネットワーク
4
ネットワーク
1
3
サービス
プロバイダ
EMD サービス
センタ
2
コンテンツ
プロバイダ

【図２】

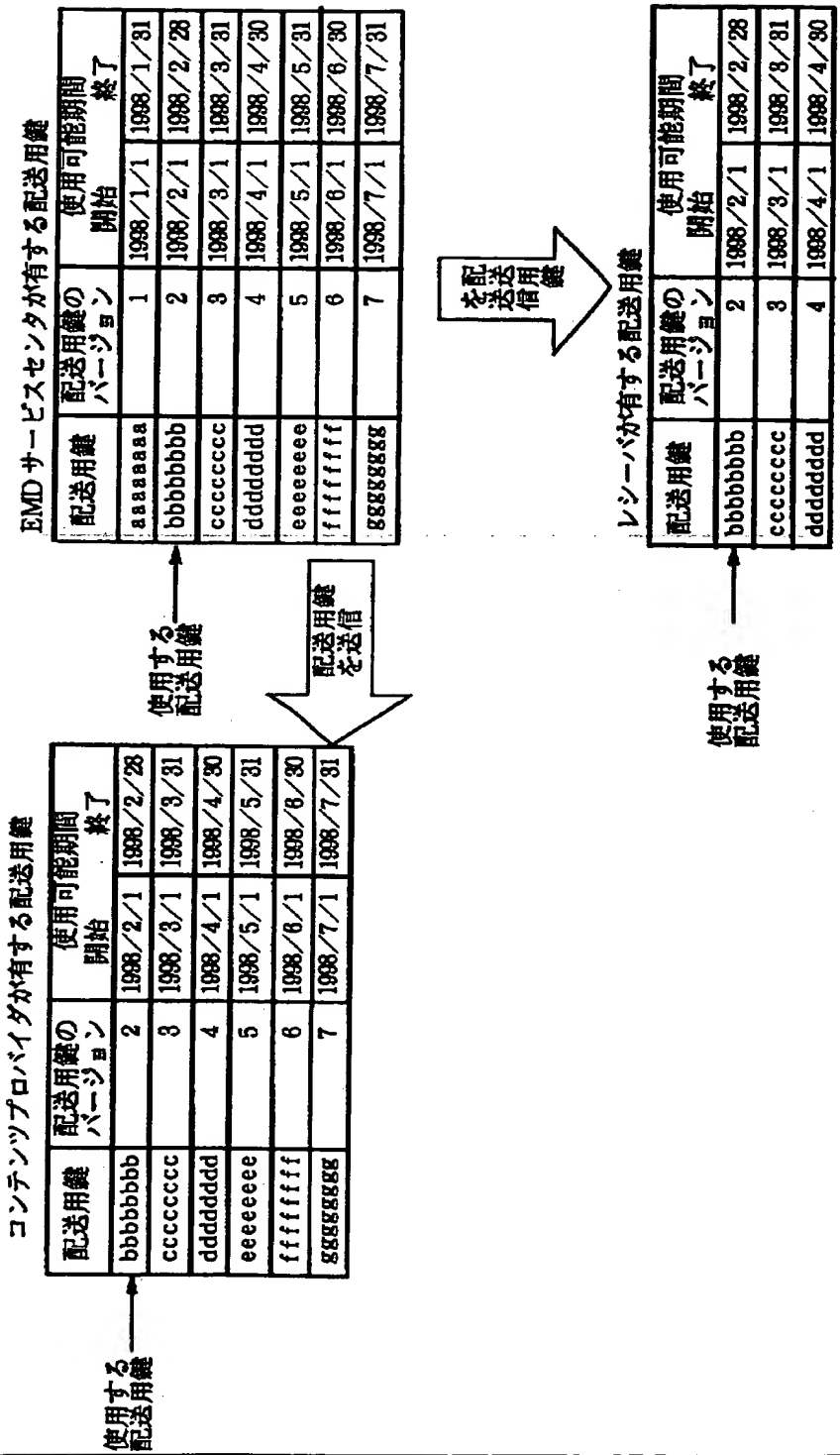


EMD サービスセンタ 1

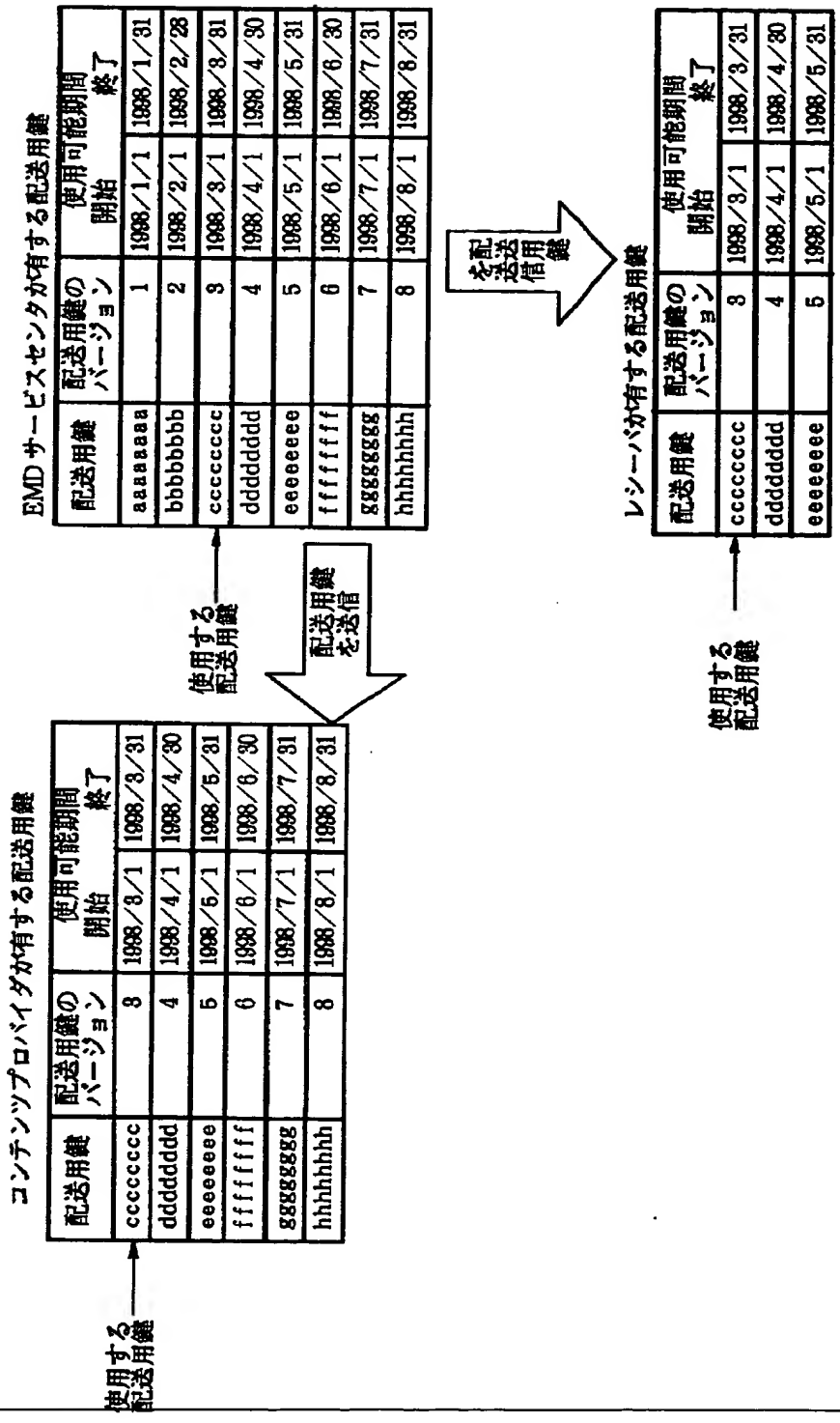
【図３】


EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵
配送用鍵を送信
配送用鍵を配送信用鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
使用する配送用鍵
コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵

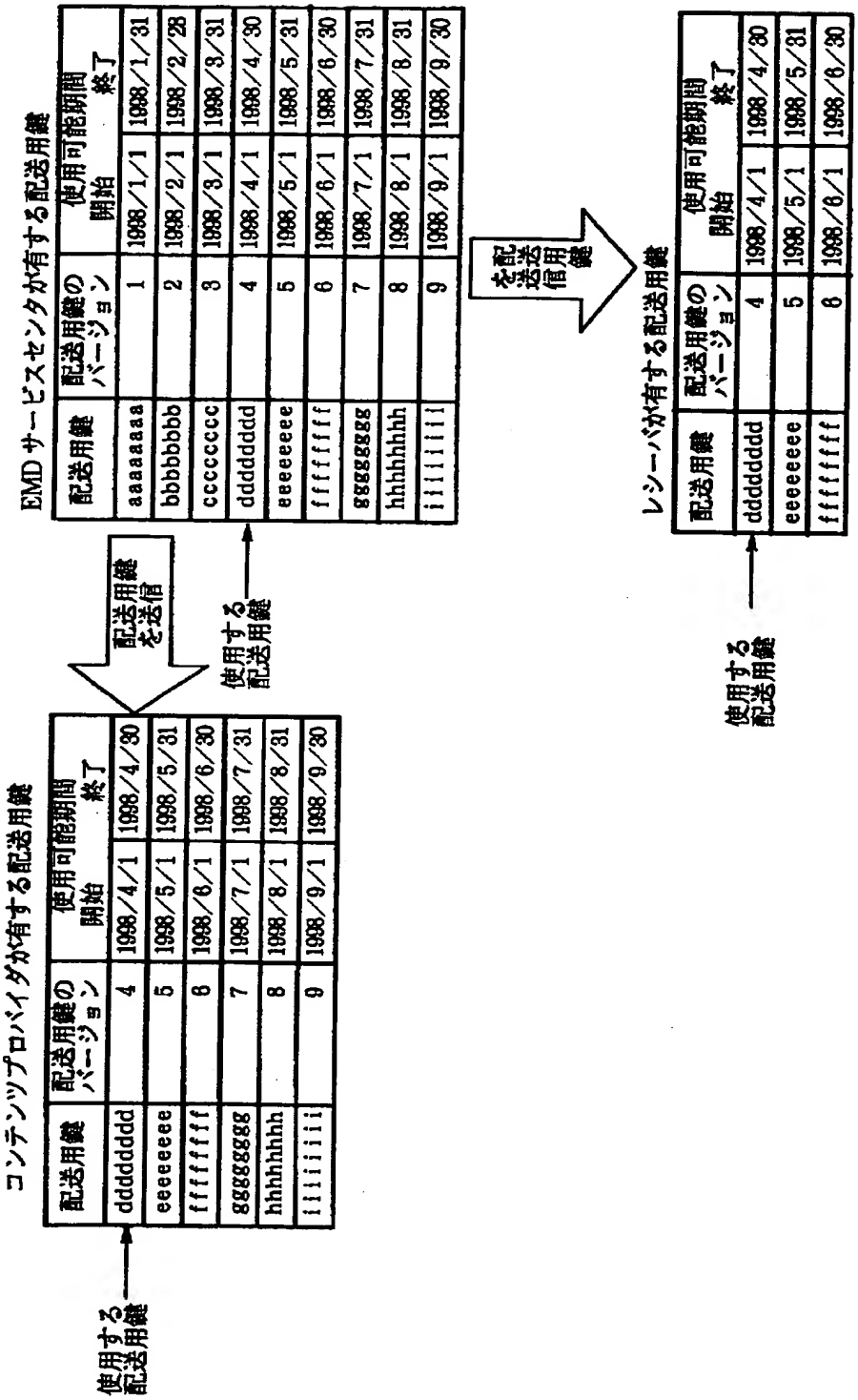
【図４】


EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
使用する配送用鍵
配送用鍵を送信
配送用鍵を送信
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
使用する配送用鍵
コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
使用する配送用鍵

【図５】


EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
使用する配送用鍵
配送用鍵を送信
コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
使用する配送用鍵
を配送信用鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
使用する配送用鍵

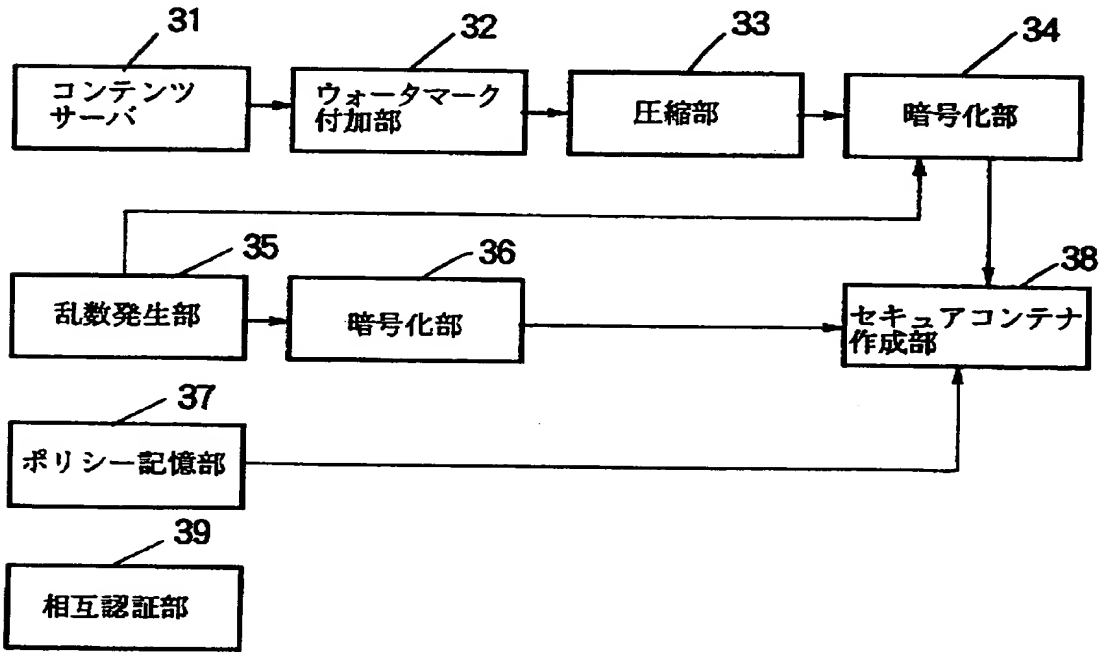
【図６】


コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
iiiiiiiii 9 1998/9/1 1998/9/30
使用する配送用鍵
配送用鍵を送信
EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
iiiiiiiii 9 1998/9/1 1998/9/30
使用する配送用鍵
配送用鍵を送信用鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵

【図７】

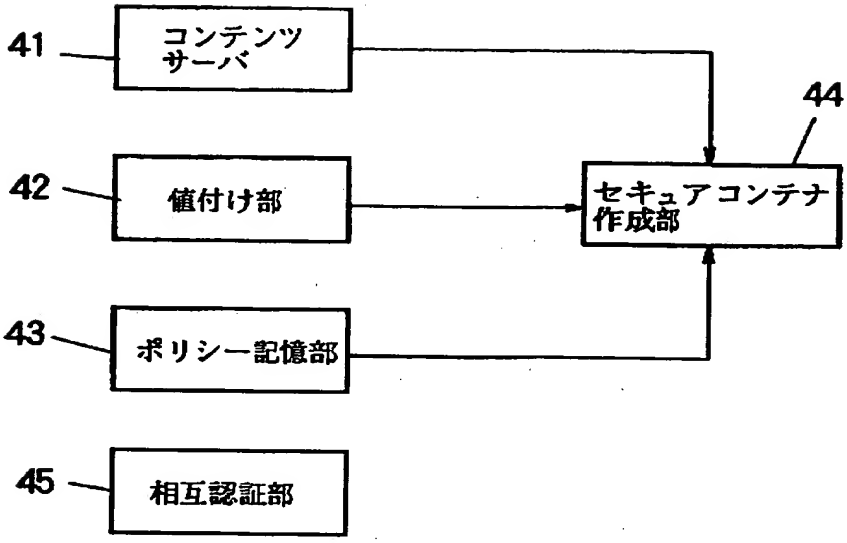
ID	決済処理	登録	EMDサービスセンタとの接続
0000000000000001h	可	可	可
0000000000000002h	可	可	不可
0000000000000003h	可	不可	可
0000000000000004h	可	不可	不可
0000000000000005h	不可	可	可
0000000000000006h	不可	可	不可
0000000000000007h	不可	不可	可
0000000000000008h	不可	不可	不可
0000000000000009h	可	可	可
•••			
FFFFFFFFFFFFFFFEh	可	不可	不可
FFFFFFFFFFFFFFFFh	不可	可	可

【図８】

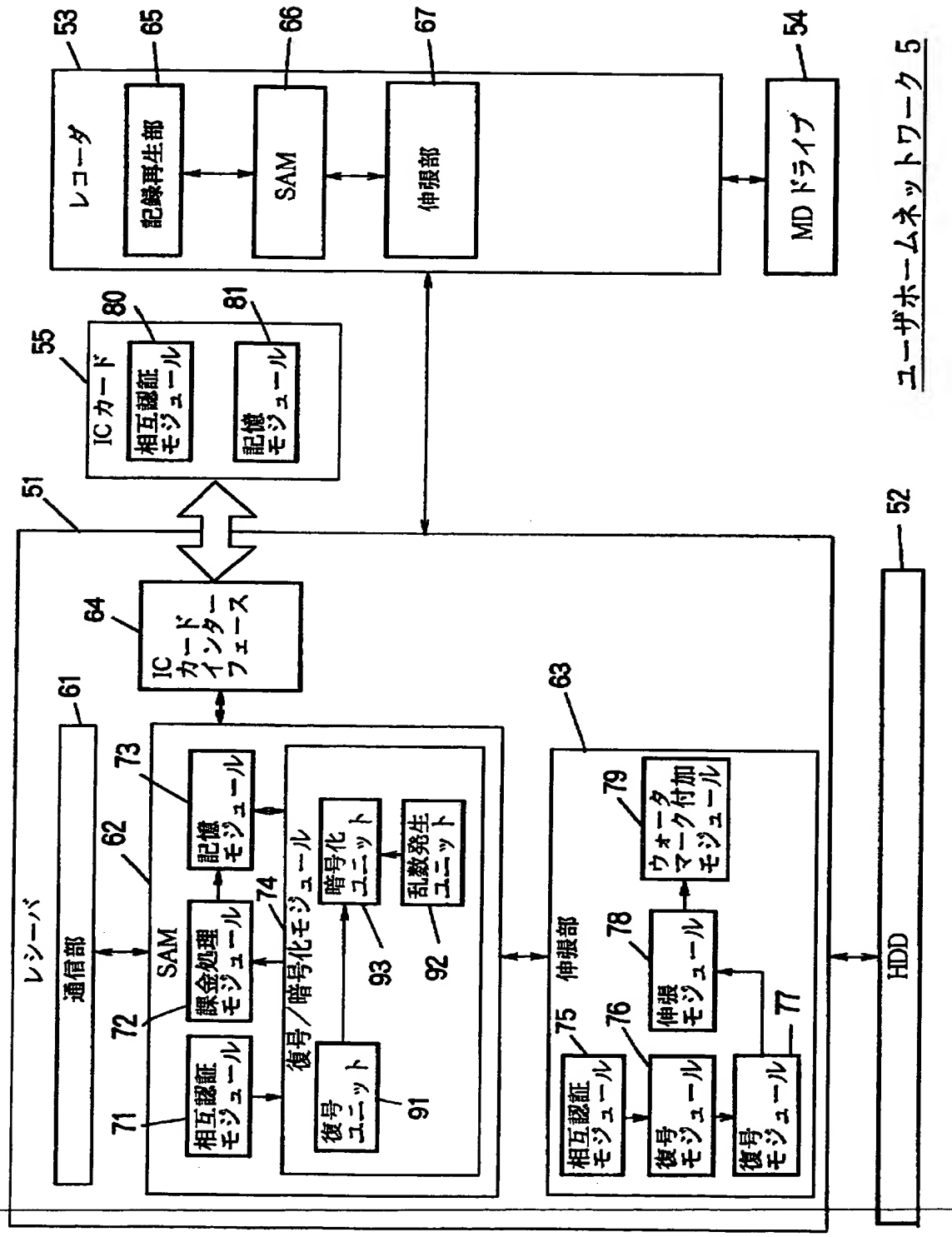


コンテンツプロバイダ 2

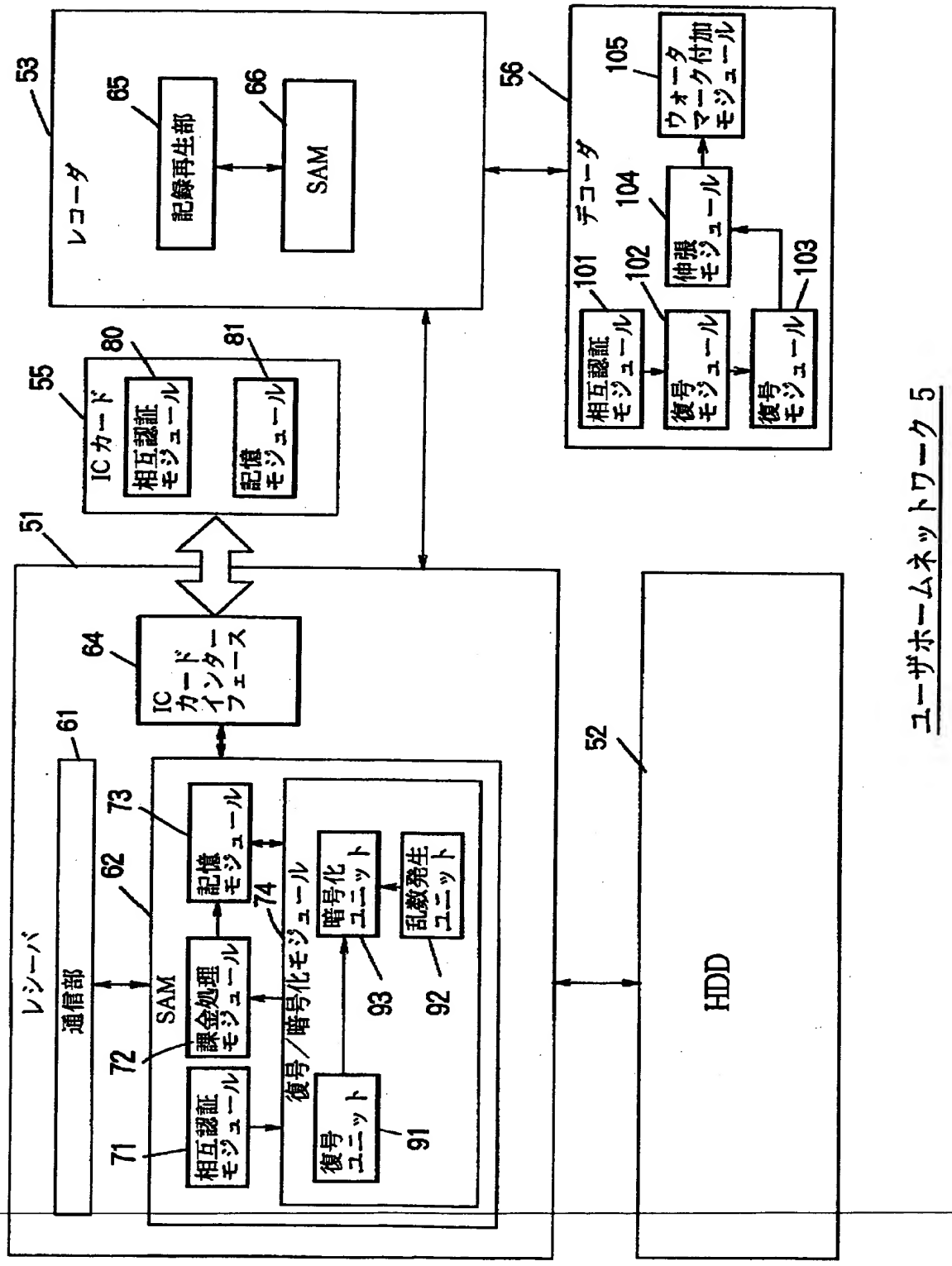
【図９】


41
コンテンツ
サーバ
42
値付け部
43
ポリシー記憶部
45
相互認証部
44
セキュアコンテナ
作成部
サービスプロバイダ３

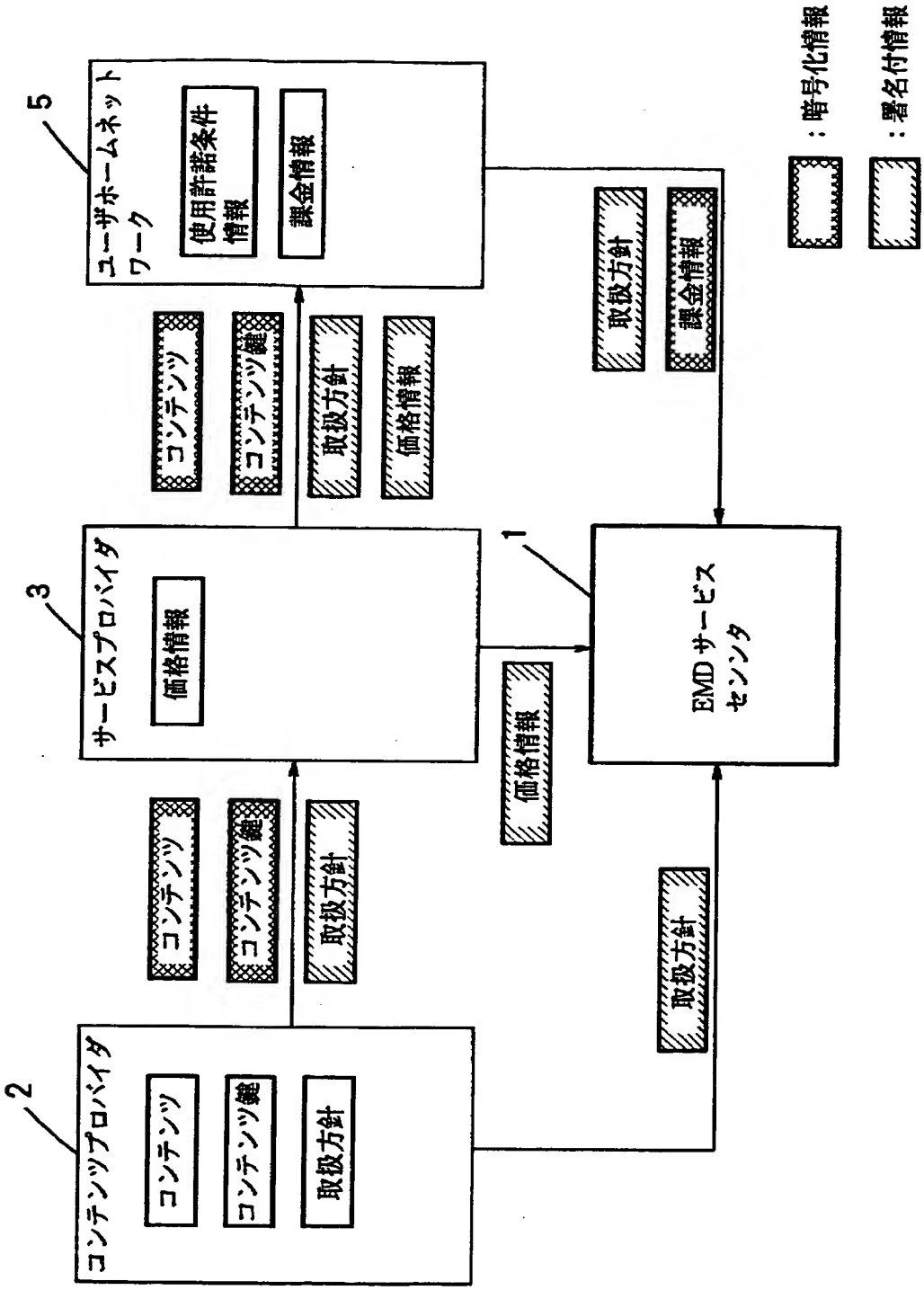
【図１０】


53
65
66
67
54
レコーダ
記録再生部
SAM
伸張部
MDドライブ
ユーザホームネットワーク5
55
80
81
ICカード
相互認証モジュール
記憶モジュール
51
52
64
ICカードインターフェース
61
63
レシーバ
通信部
62
73
79
ウォークマーク付加モジュール
SAM
課金処理モジュール
記憶モジュール
暗号化ユニット
乱数発生ユニット
74
復号／暗号化モジュール
伸張部
78
72
93
92
71
相互認証モジュール
復号ユニット
91
75
76
77
相互認証モジュール
復号モジュール
伸張モジュール
復号モジュール
HDD

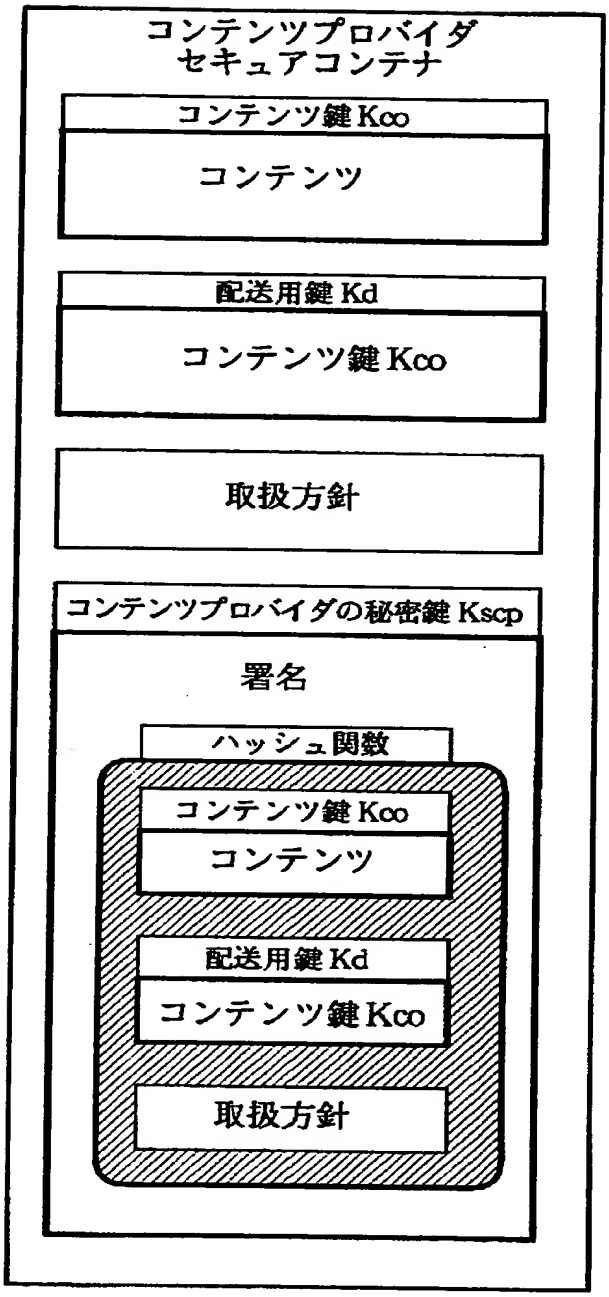
【図１１】


53
レコーダ
85
記録再生部
66
SAM
56
デコーダ
105
ウォータマーク付加モジュール
104
伸張モジュール
101
相互認証モジュール
102
復号モジュール
103
復号モジュール
55
ICカード
80
相互認証モジュール
81
記憶モジュール
51
64
ICカードインターフェース
61
レシーバ
通信部
62
SAM
73
記憶モジュール
74
復号／暗号化モジュール
暗号化ユニット
乱数発生ユニット
93
92
課金処理モジュール
72
相互認証モジュール
71
復号ユニット
91
52
HDD
ユーザホームネットワーク５

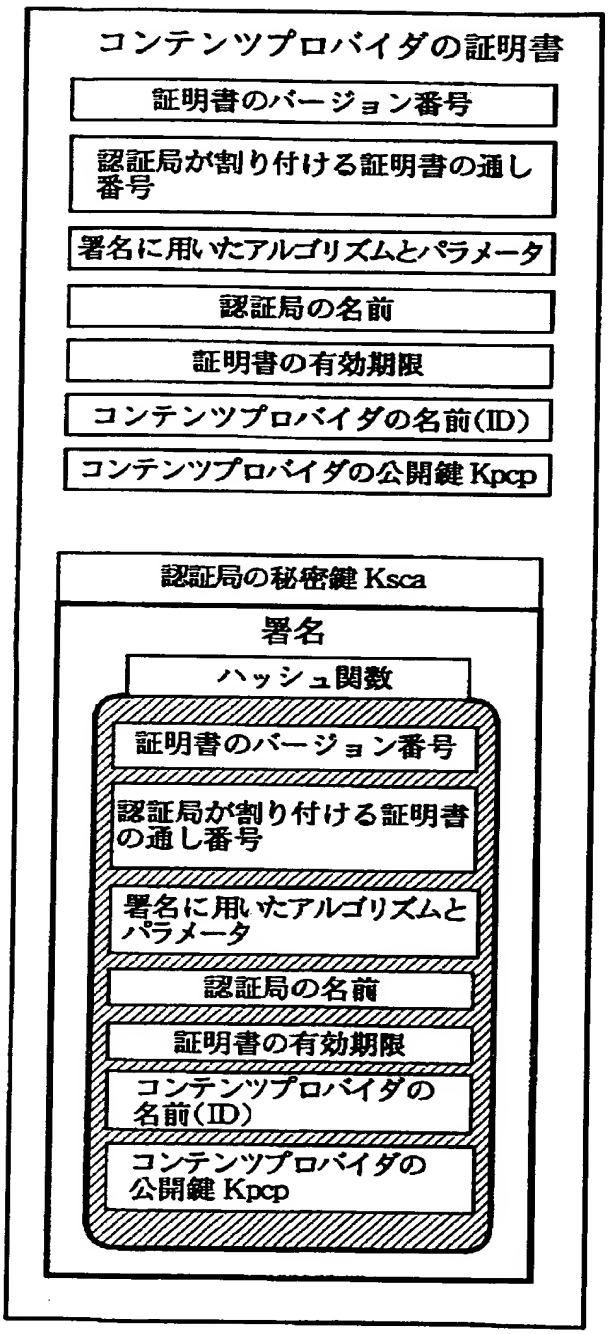
【図１２】


：暗号化情報
：署名付情報
5
ユーザホームネットワーク
使用許諾条件情報
課金情報
コンテンツ
コンテンツ鍵
取扱方針
価格情報
取扱方針
課金情報
3
サービスプロバイダ
価格情報
1
EMDサービスセンタ
価格情報
コンテンツ
コンテンツ鍵
取扱方針
取扱方針
2
コンテンツプロバイダ
コンテンツ
コンテンツ鍵
取扱方針

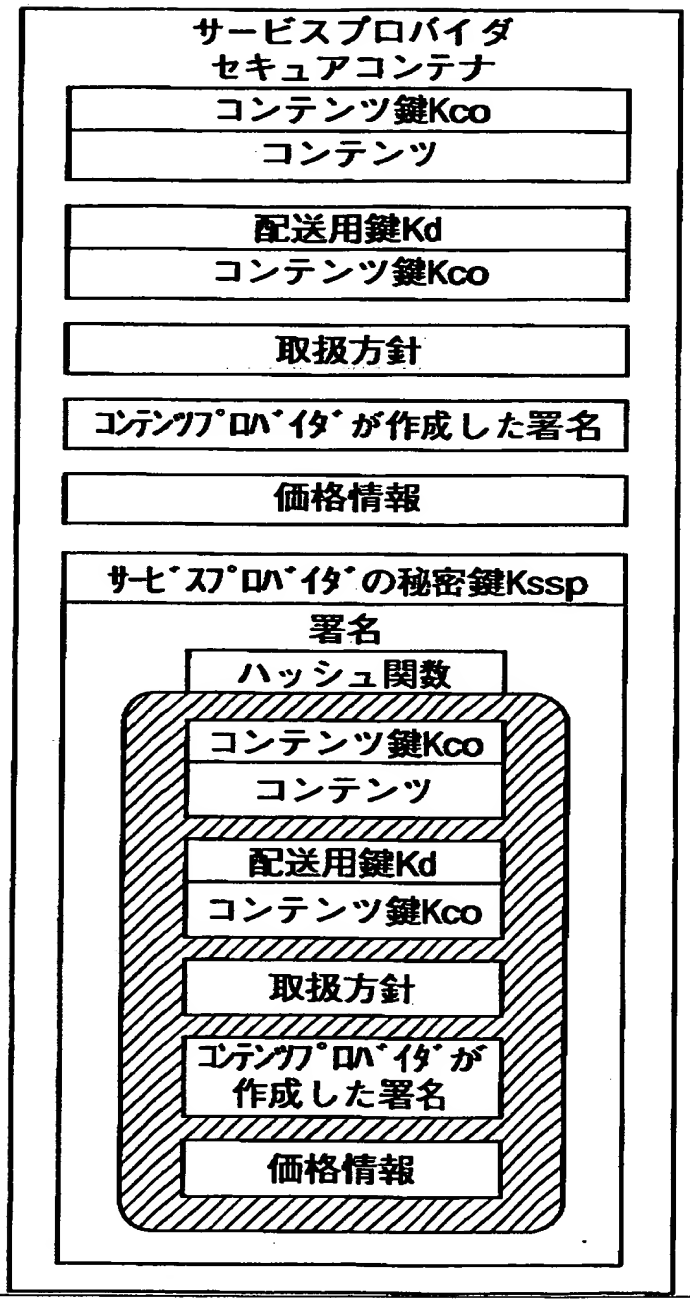
【図１３】


コンテンツプロバイダ
セキュアコンテナ
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
取扱方針
コンテンツプロバイダの秘密鍵 Kscp
署名
ハッシュ関数
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
取扱方針

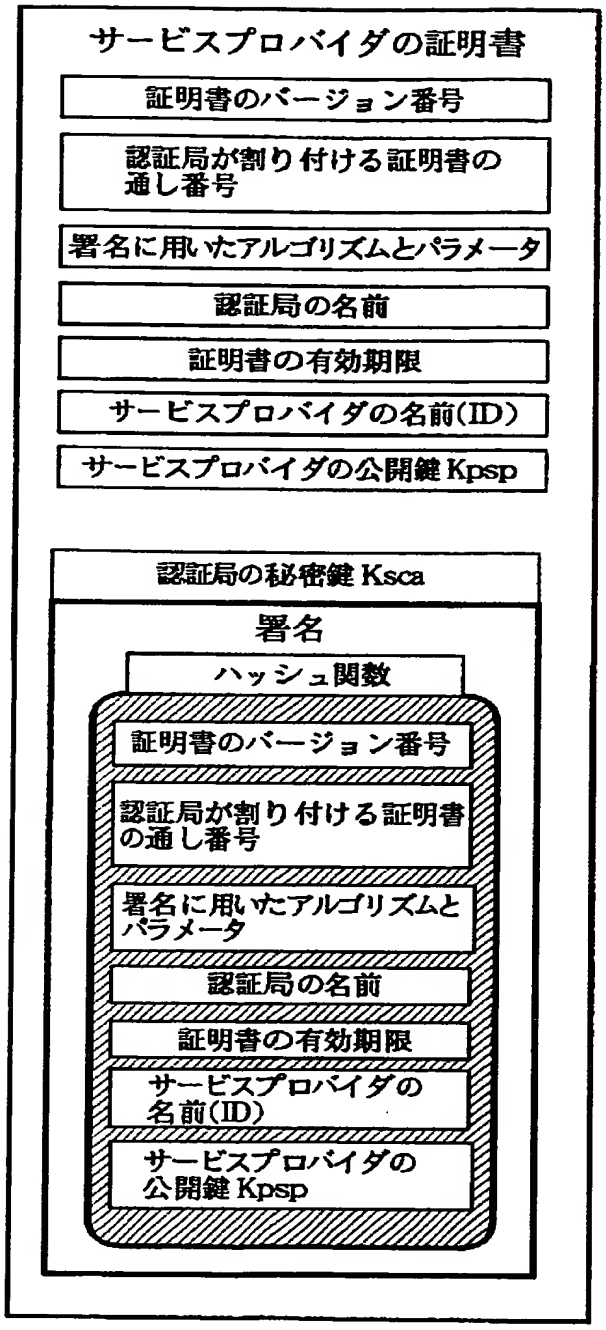
【図１４】


コンテンツプロバイダの証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
コンテンツプロバイダの名前(ID)
コンテンツプロバイダの公開鍵 Kpcp
認証局の秘密鍵 Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
コンテンツプロバイダの名前(ID)
コンテンツプロバイダの公開鍵 Kpcp

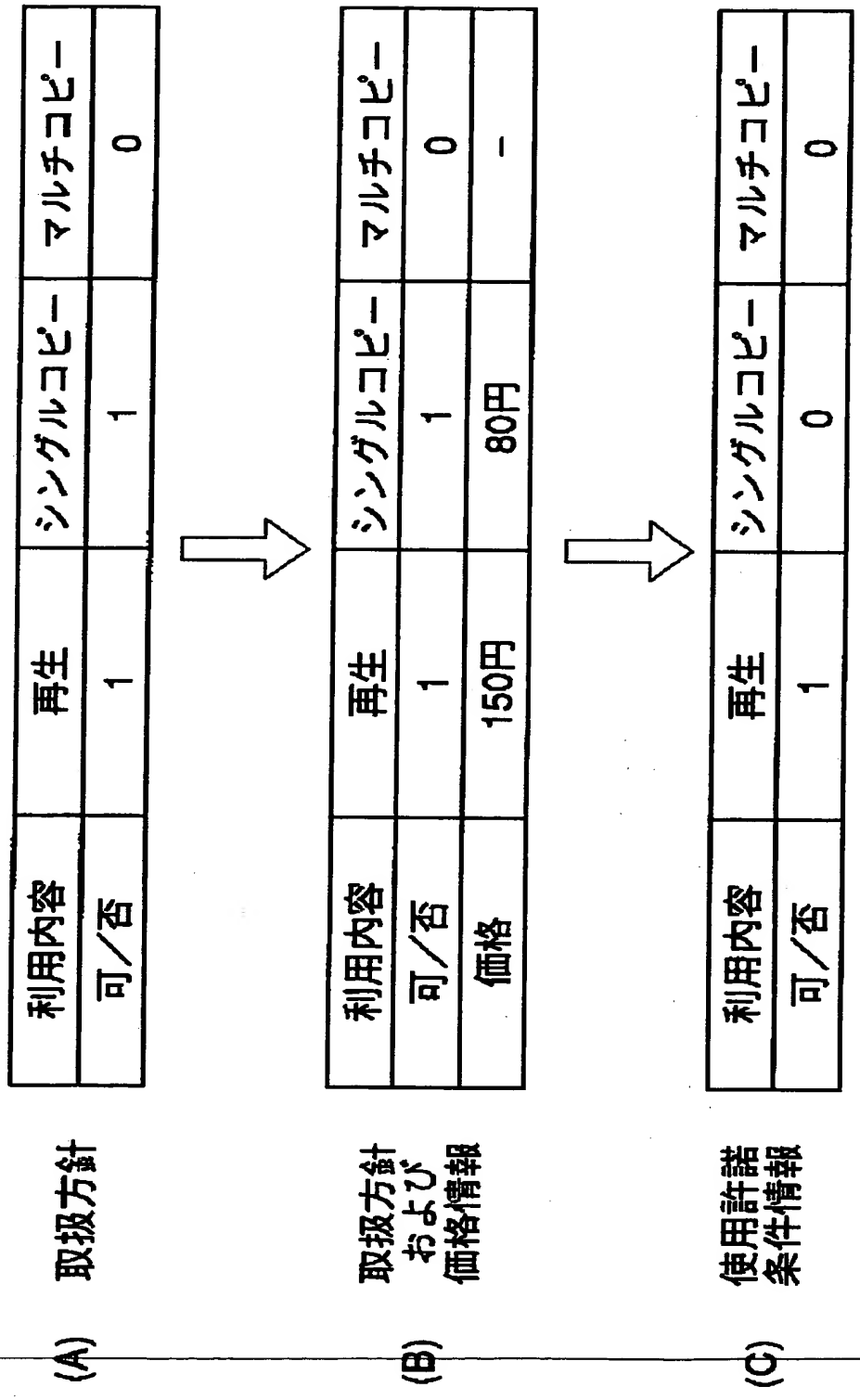
【図１５】


サービスプロバイダ
セキュアコンテナ
コンテンツ鍵Kco
コンテンツ
配送用鍵Kd
コンテンツ鍵Kco
取扱方針
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞが作成した署名
価格情報
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞの秘密鍵Kssp
署名
ハッシュ関数
コンテンツ鍵Kco
コンテンツ
配送用鍵Kd
コンテンツ鍵Kco
取扱方針
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞが
作成した署名
価格情報

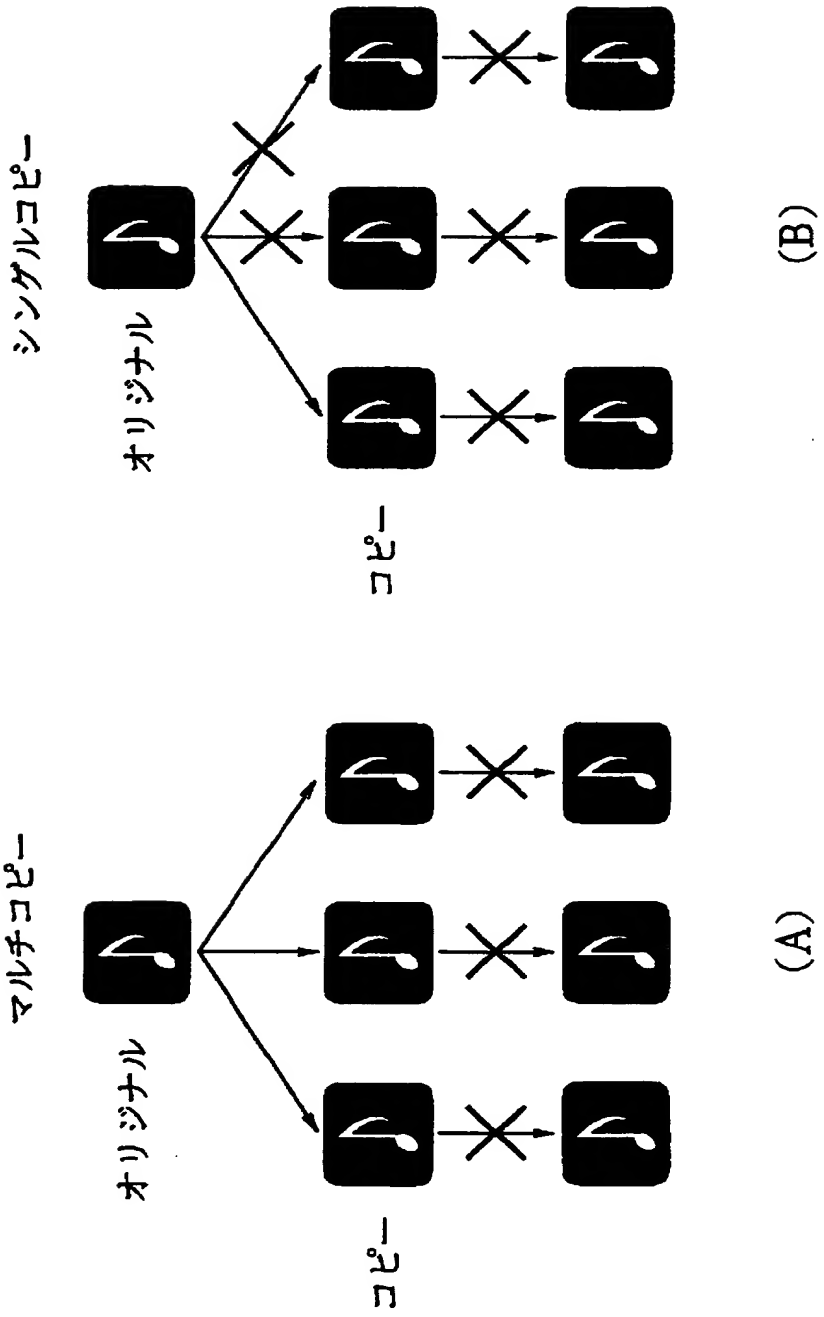
【図１６】


サービスプロバイダの証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
サービスプロバイダの名前(ID)
サービスプロバイダの公開鍵 Kpsp
認証局の秘密鍵 Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
サービスプロバイダの名前(ID)
サービスプロバイダの公開鍵 Kpsp

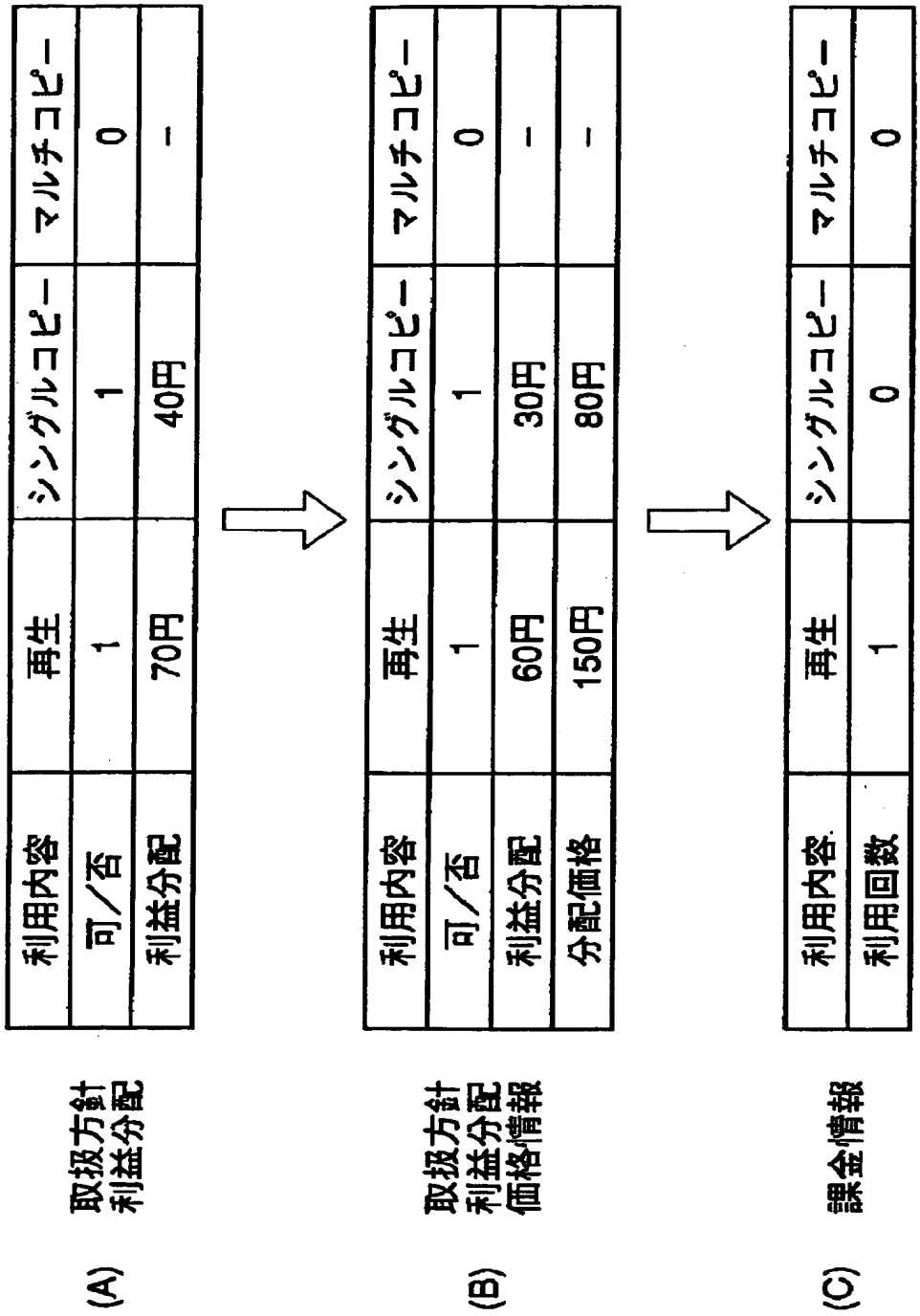
【図１７】


(A) 取扱方針
利用内容
可／否
再生
1
シングルコピー
1
マルチコピー
0
(B) 取扱方針および価格情報
利用内容
可／否
価格
再生
1
150円
シングルコピー
1
80円
マルチコピー
0
–
(C) 使用許諾条件情報
利用内容
可／否
再生
1
シングルコピー
0
マルチコピー
0

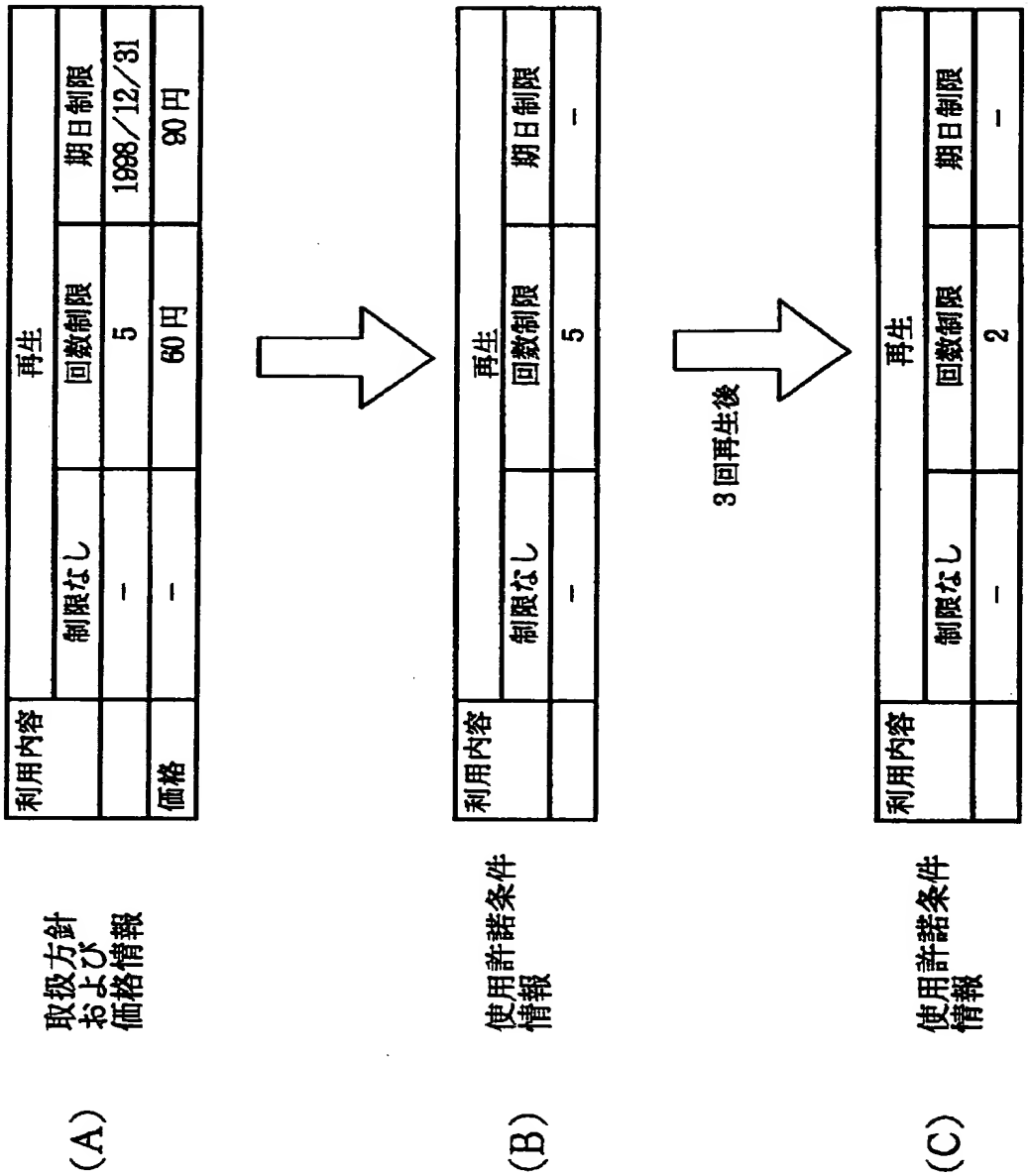
【図１８】



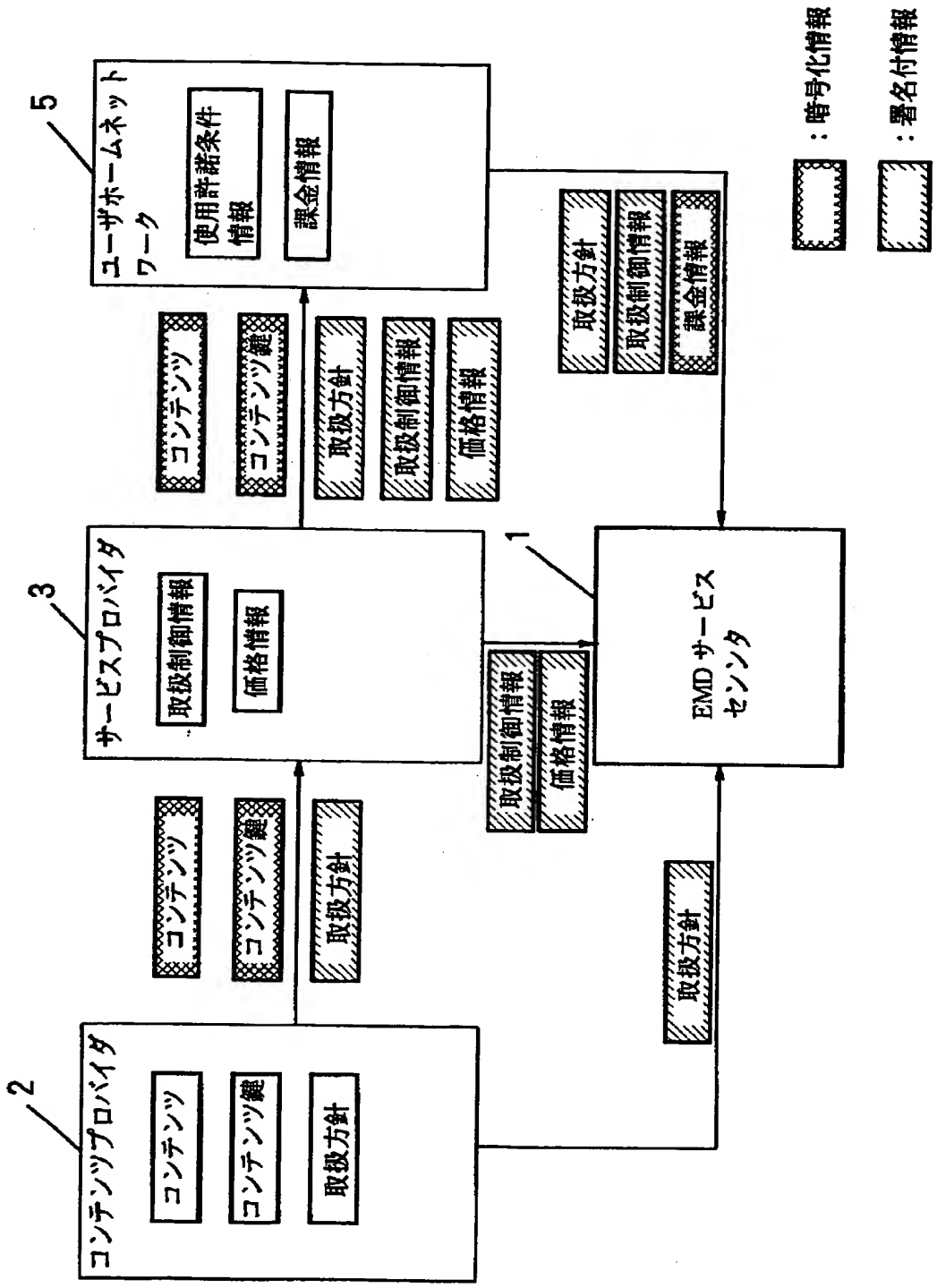
【図１９】


利用内容
可／否
利益分配
再生
1
70円
シングルコピー
1
40円
マルチコピー
0
－
(A)
取扱方針
利益分配
利用内容
可／否
利益分配
分配価格
再生
1
60円
150円
シングルコピー
1
30円
80円
マルチコピー
0
－
－
(B)
取扱方針
利益分配
価格情報
利用内容
利用回数
再生
1
シングルコピー
0
マルチコピー
0
(C)
課金情報

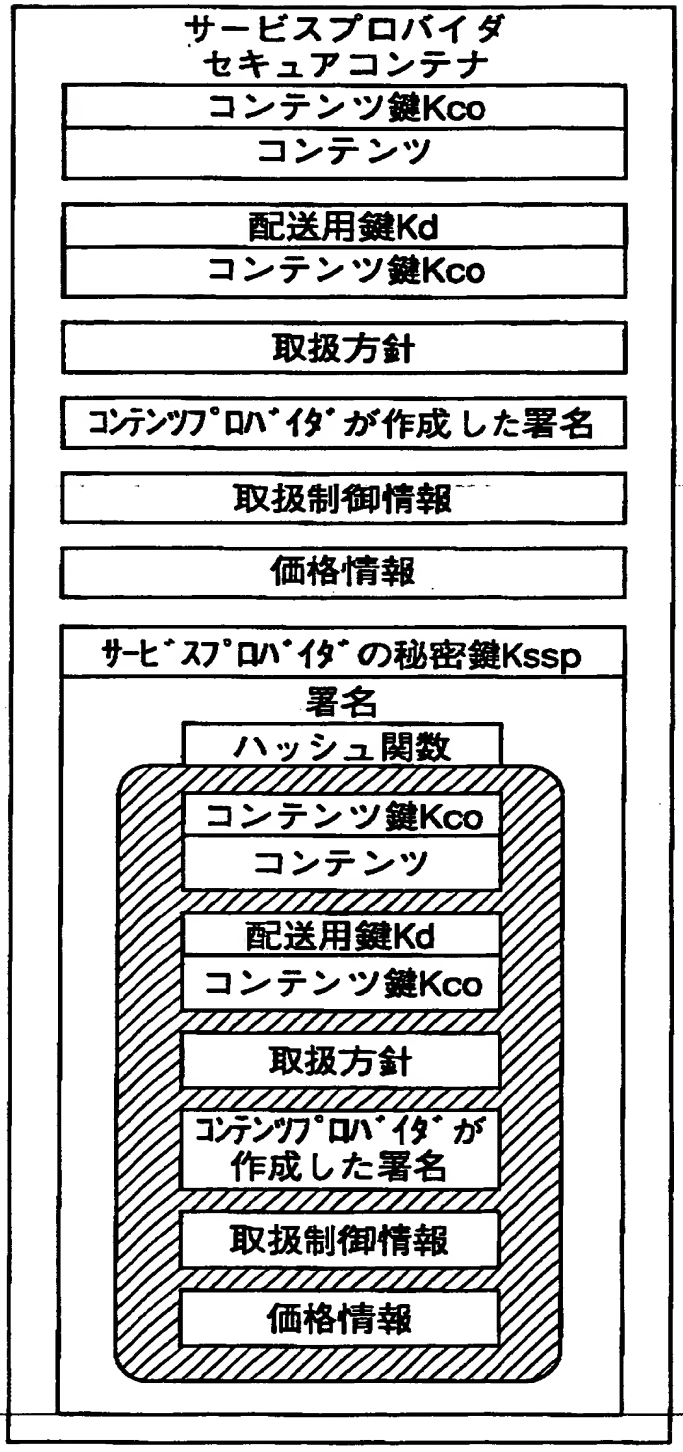
【図２０】


(A)
取扱方針および価格情報
利用内容
再生
制限なし
回数制限
期日制限
－
5
1998／12／31
価格
－
60円
90円
(B)
使用許諾条件情報
利用内容
再生
制限なし
回数制限
期日制限
－
5
－
3回再生後
(C)
使用許諾条件情報
利用内容
再生
制限なし
回数制限
期日制限
－
2
－

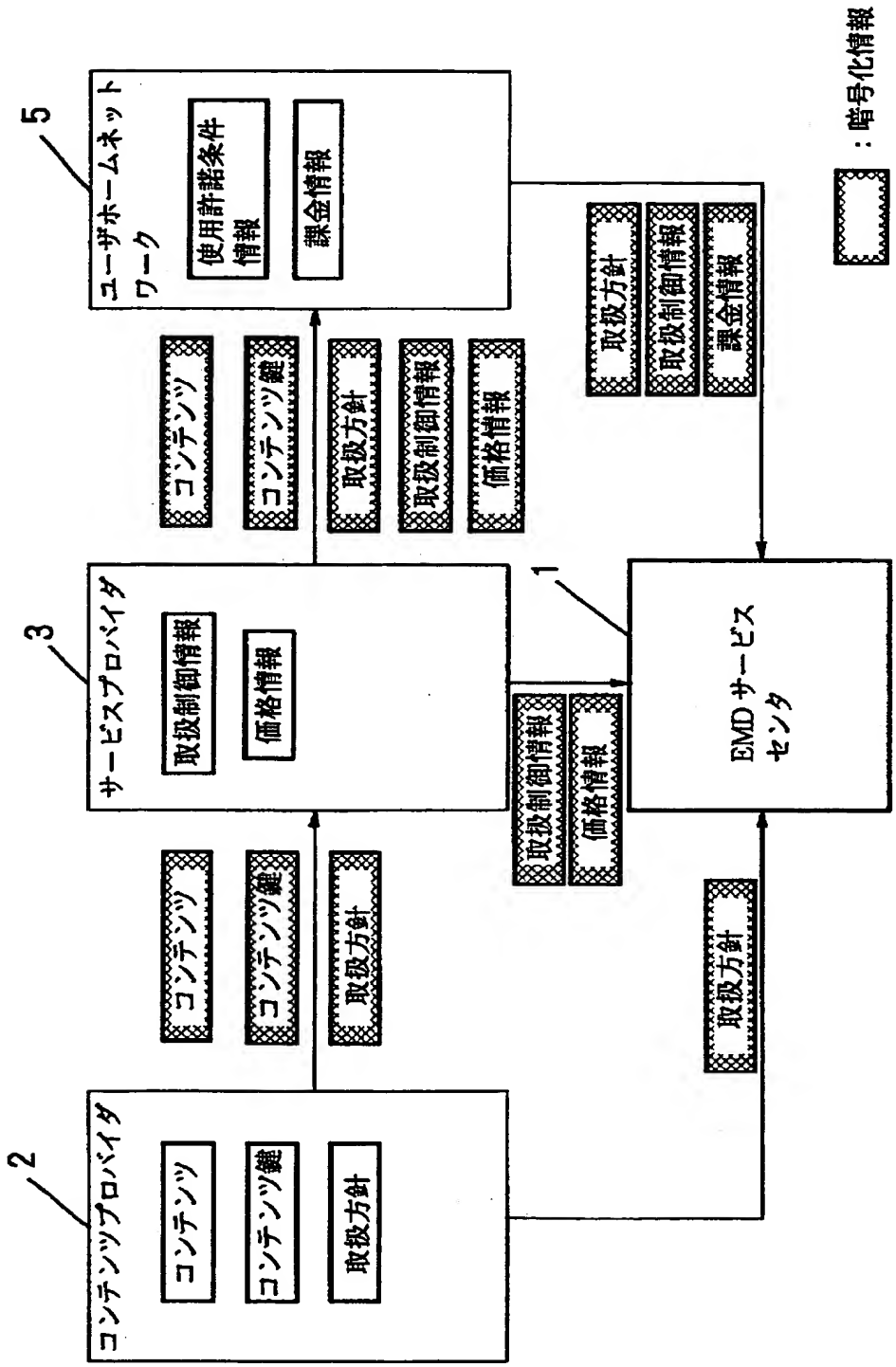
【図２１】


5
ユーザホームネットワーク
使用許諾条件情報
課金情報
3
サービスプロバイダ
取扱制御情報
価格情報
2
コンテンツプロバイダ
コンテンツ
コンテンツ鍵
取扱方針
1
EMDサービスセンタ
コンテンツ
コンテンツ鍵
取扱方針
取扱制御情報
価格情報
取扱方針
取扱制御情報
課金情報
取扱方針
：暗号化情報
：署名付情報

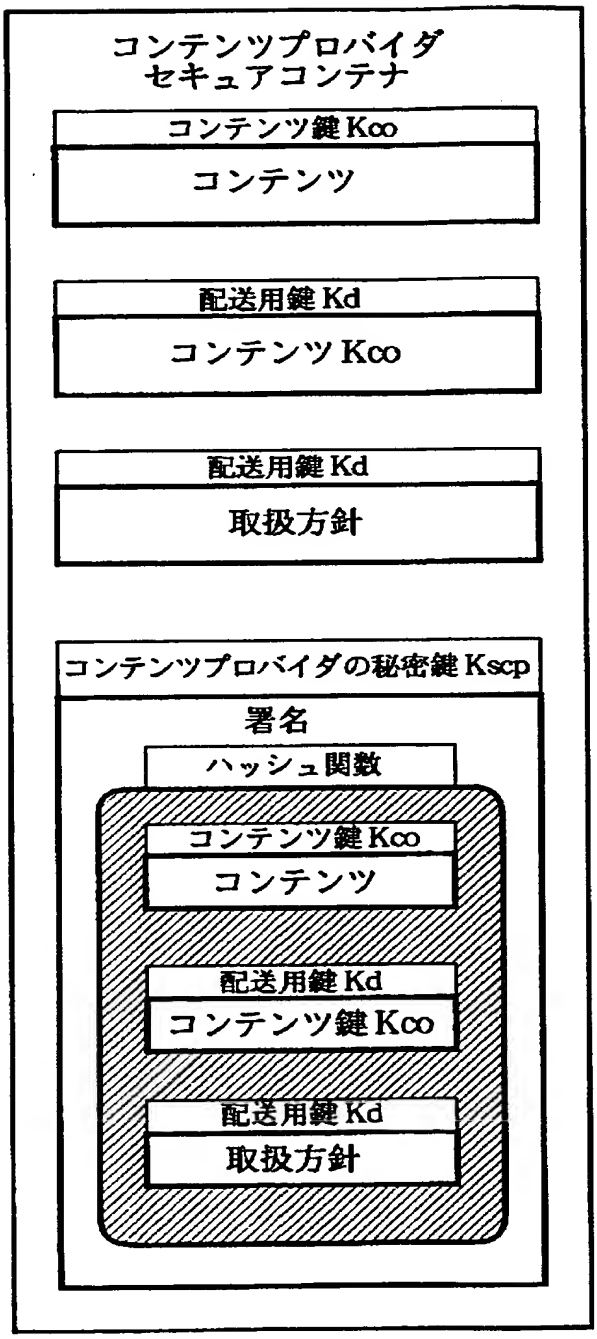
【図２２】


サービスプロバイダ
セキュアコンテナ
コンテンツ鍵Kco
コンテンツ
配送用鍵Kd
コンテンツ鍵Kco
取扱方針
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞが作成した署名
取扱制御情報
価格情報
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞの秘密鍵Kssp
署名
ハッシュ関数
コンテンツ鍵Kco
コンテンツ
配送用鍵Kd
コンテンツ鍵Kco
取扱方針
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞが
作成した署名
取扱制御情報
価格情報

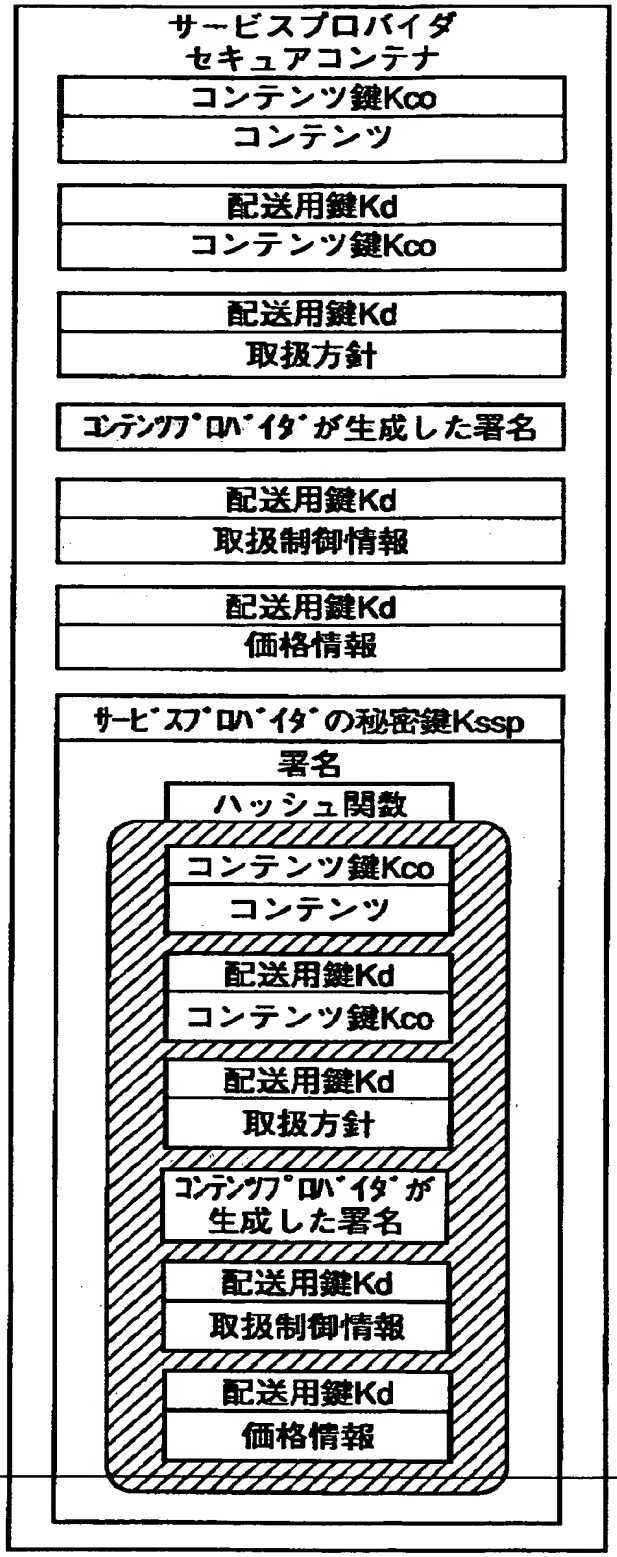
【図２４】


：暗号化情報
5
ユーザホームネットワーク
使用許諾条件情報
課金情報
3
サービスプロバイダ
取扱制御情報
価格情報
2
コンテンツプロバイダ
コンテンツ
コンテンツ鍵
取扱方針
1
EMD サービスセンタ
コンテンツ
コンテンツ鍵
取扱方針
取扱制御情報
価格情報
取扱方針
取扱制御情報
価格情報
取扱方針
取扱制御情報
課金情報

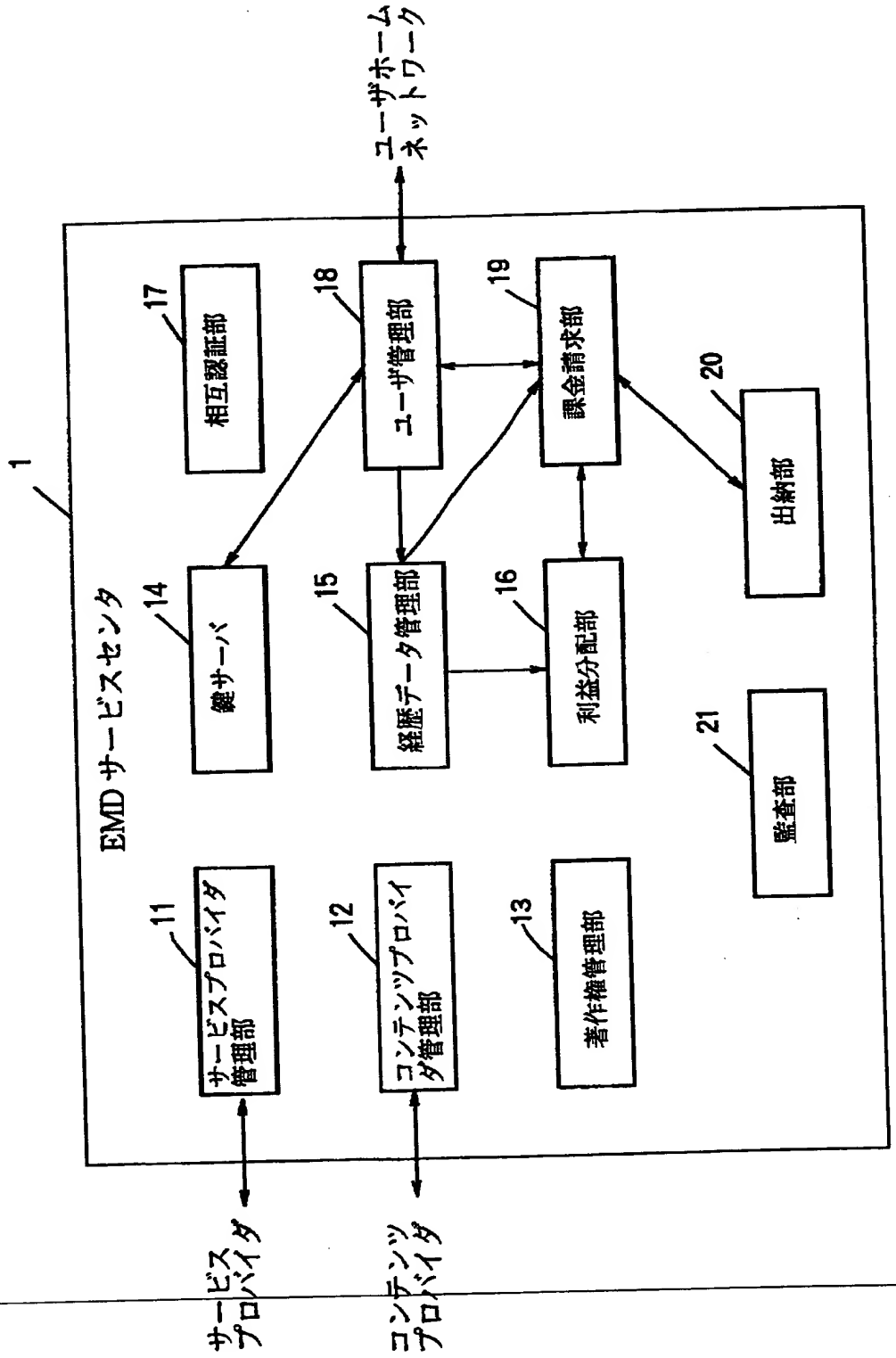
【図２５】


コンテンツプロバイダ
セキュアコンテナ
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ Kco
配送用鍵 Kd
取扱方針
コンテンツプロバイダの秘密鍵 Kscp
署名
ハッシュ関数
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
配送用鍵 Kd
取扱方針

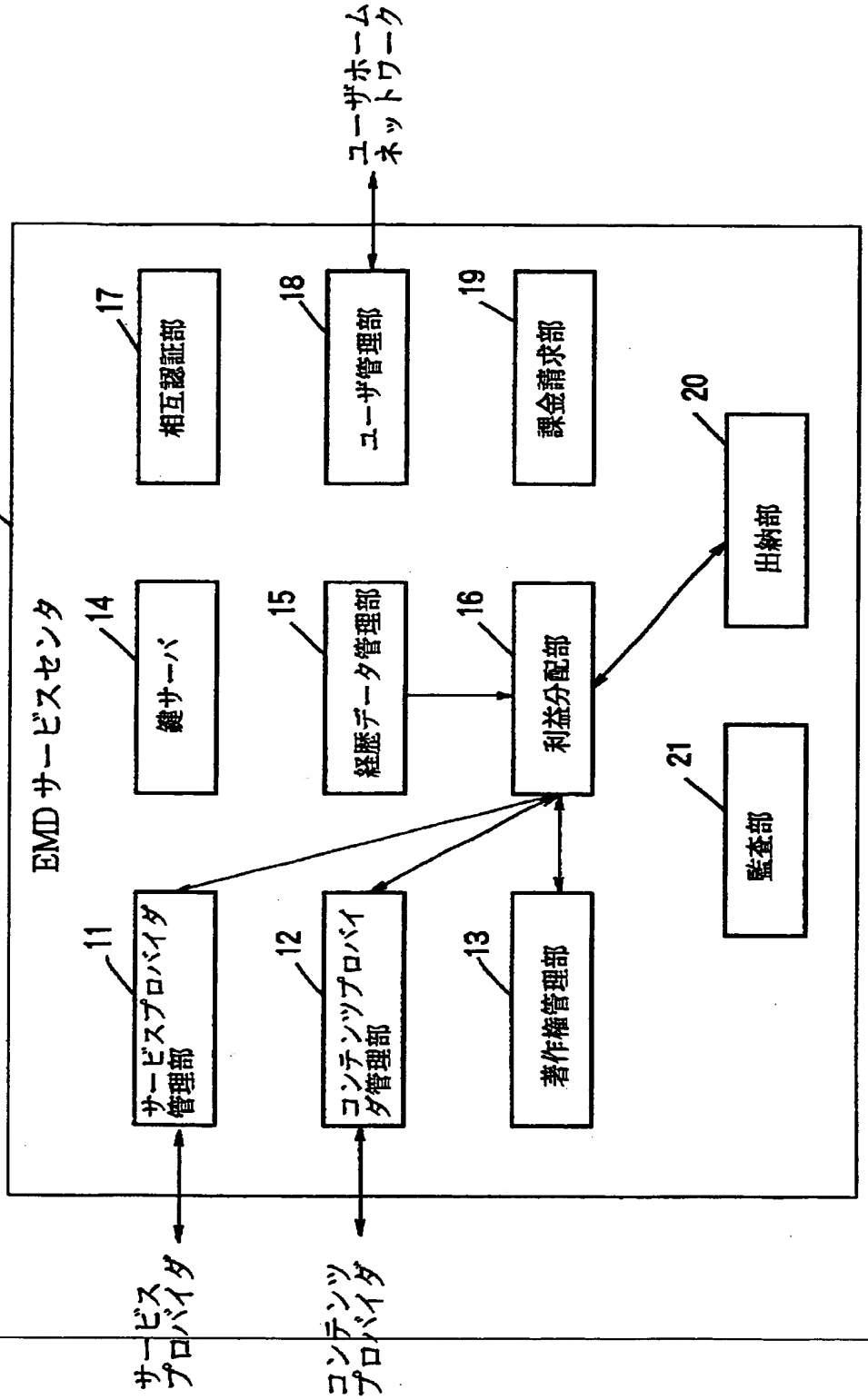
【図２６】


サービスプロバイダ
セキュアコンテナ
コンテンツ鍵Kco
コンテンツ
配送用鍵Kd
コンテンツ鍵Kco
配送用鍵Kd
取扱方針
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞが生成した署名
配送用鍵Kd
取扱制御情報
配送用鍵Kd
価格情報
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞの秘密鍵Kssp
署名
ハッシュ関数
コンテンツ鍵Kco
コンテンツ
配送用鍵Kd
コンテンツ鍵Kco
配送用鍵Kd
取扱方針
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞが
生成した署名
配送用鍵Kd
取扱制御情報
配送用鍵Kd
価格情報

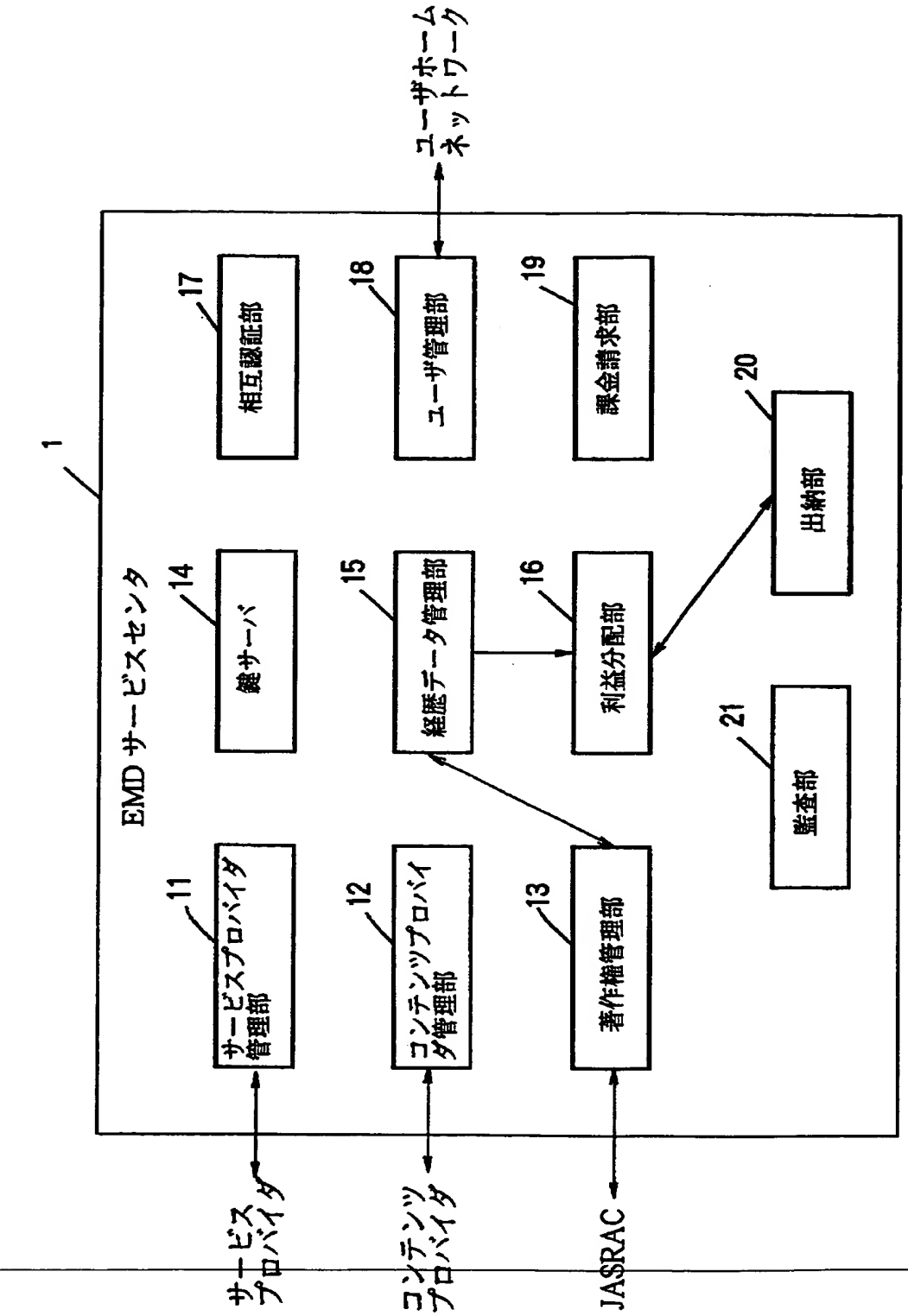
【図２７】


ユーザホーム
ネットワーク
1
EMDサービスセンタ
17
相互認証部
18
ユーザ管理部
19
課金請求部
20
出納部
14
鍵サーバ
15
経歴データ管理部
16
利益分配部
21
監査部
11
サービスプロバイダ
管理部
12
コンテンツプロバイ
ダ管理部
13
著作権管理部
サービス
プロバイダ
コンテンツ
プロバイダ

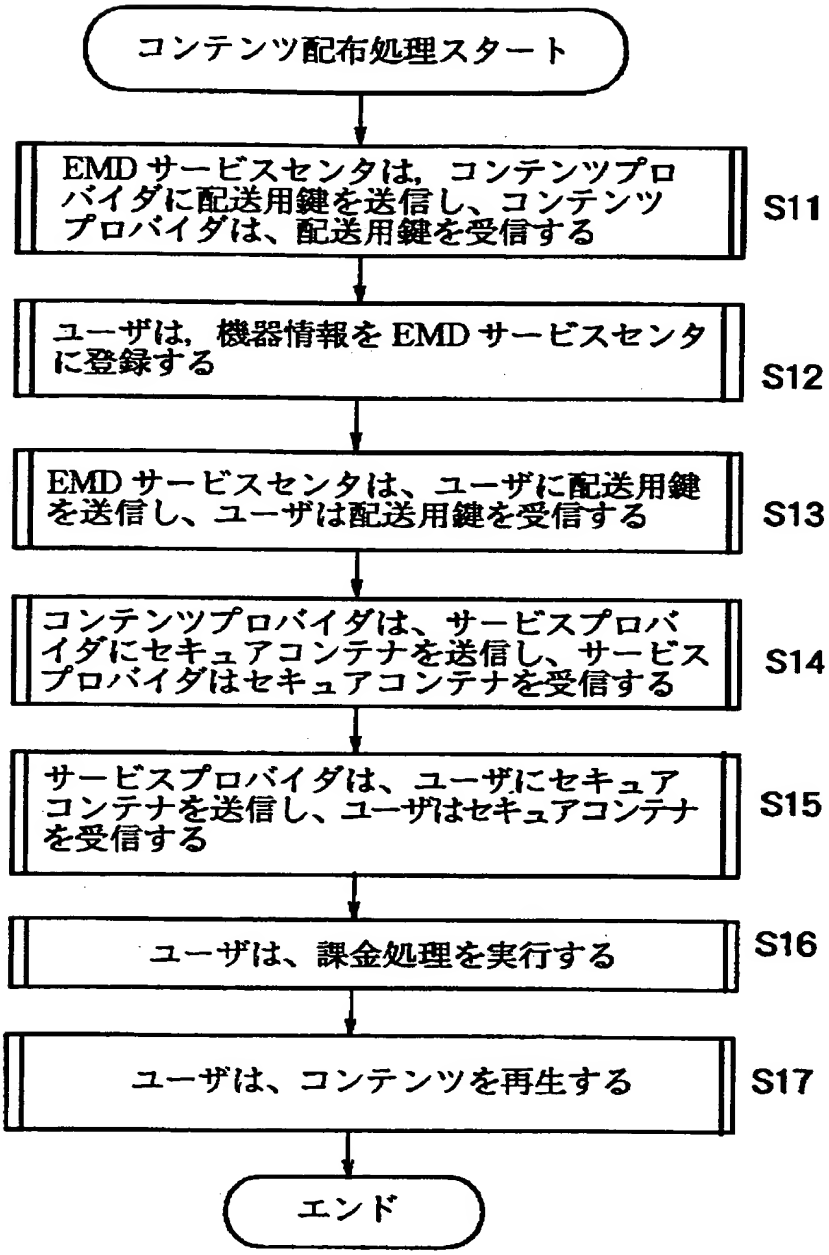
【図２８】


ユーザホームネットワーク
1
EMD サービスセンタ
17
相互認証部
18
ユーザ管理部
19
課金請求部
20
出納部
14
鍵サーバ
15
経歴データ管理部
16
利益分配部
21
監査部
11
サービスプロバイダ管理部
12
コンテンツプロバイダ管理部
13
著作権管理部
サービスプロバイダ
コンテンツプロバイダ

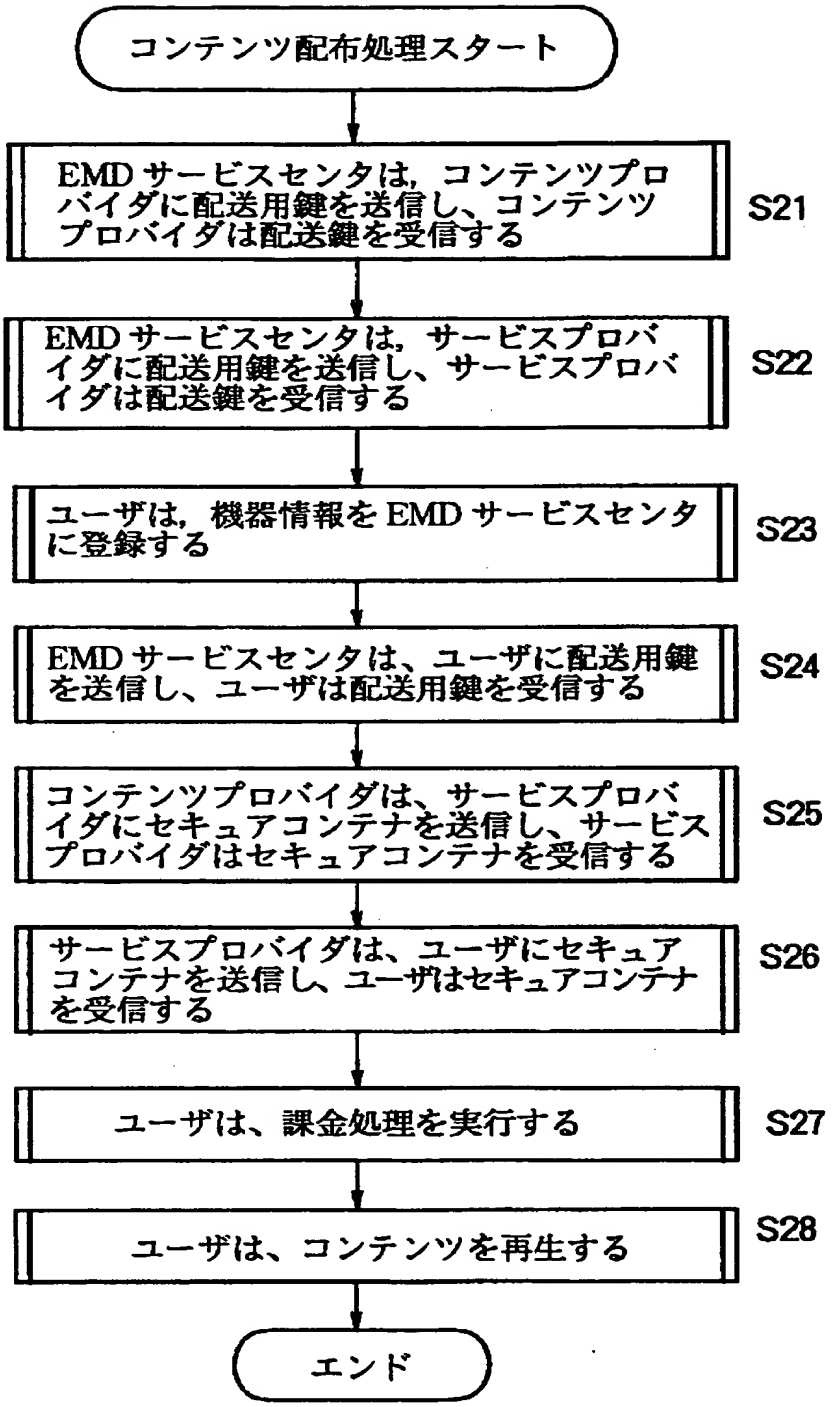
【図２９】


ユーザホームネットワーク
1
EMD サービスセンタ
17
相互認証部
18
ユーザ管理部
19
課金請求部
20
出納部
14
鍵サーバ
15
経歴データ管理部
16
利益分配部
21
監査部
11
サービスプロバイダ管理部
12
コンテンツプロバイダ管理部
13
著作権管理部
サービスプロバイダ
コンテンツプロバイダ
JASRAC

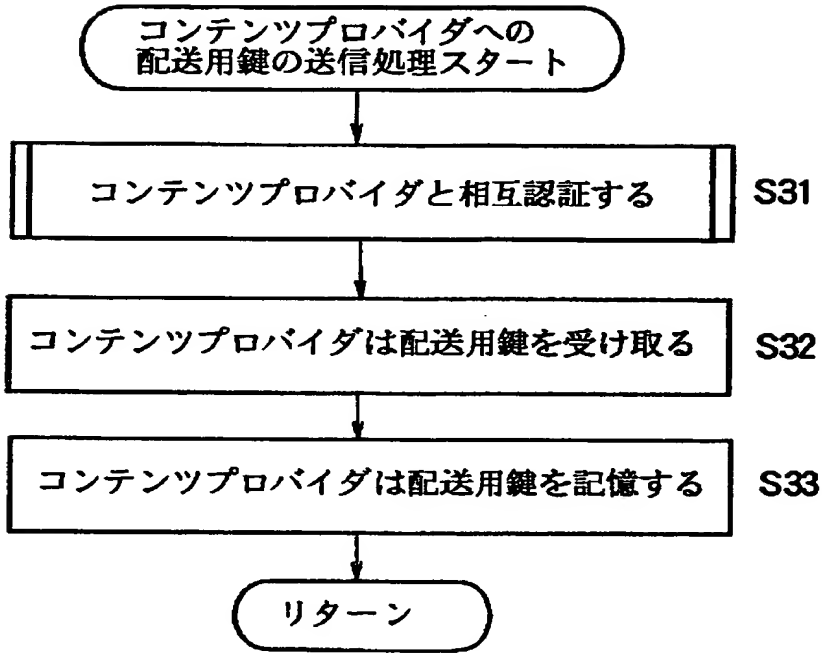
【図３０】


コンテンツ配布処理スタート
EMDサービスセンタは，コンテンツプロバイダに配送用鍵を送信し、コンテンツプロバイダは、配送用鍵を受信する
S11
ユーザは，機器情報をEMDサービスセンタに登録する
S12
EMDサービスセンタは、ユーザに配送用鍵を送信し、ユーザは配送用鍵を受信する
S13
コンテンツプロバイダは、サービスプロバイダにセキュアコンテナを送信し、サービスプロバイダはセキュアコンテナを受信する
S14
サービスプロバイダは、ユーザにセキュアコンテナを送信し、ユーザはセキュアコンテナを受信する
S15
ユーザは、課金処理を実行する
S16
ユーザは、コンテンツを再生する
S17
エンド

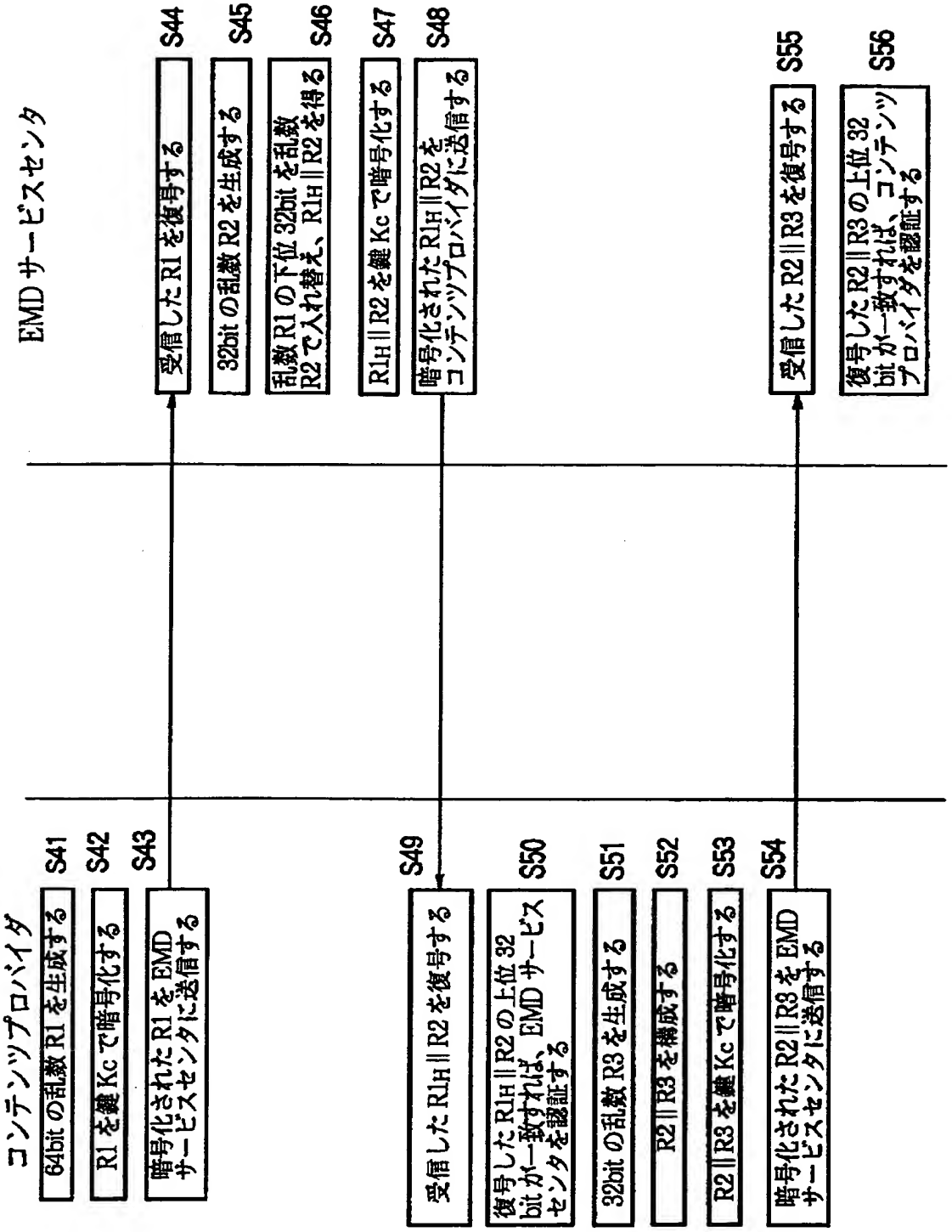
【図３１】


コンテンツ配布処理スタート
EMDサービスセンタは，コンテンツプロバイダに配送用鍵を送信し、コンテンツプロバイダは配送鍵を受信する
S21
EMDサービスセンタは，サービスプロバイダに配送用鍵を送信し、サービスプロバイダは配送鍵を受信する
S22
ユーザは，機器情報をEMDサービスセンタに登録する
S23
EMDサービスセンタは、ユーザに配送用鍵を送信し、ユーザは配送用鍵を受信する
S24
コンテンツプロバイダは、サービスプロバイダにセキュアコンテナを送信し、サービスプロバイダはセキュアコンテナを受信する
S25
サービスプロバイダは、ユーザにセキュアコンテナを送信し、ユーザはセキュアコンテナを受信する
S26
ユーザは、課金処理を実行する
S27
ユーザは、コンテンツを再生する
S28
エンド

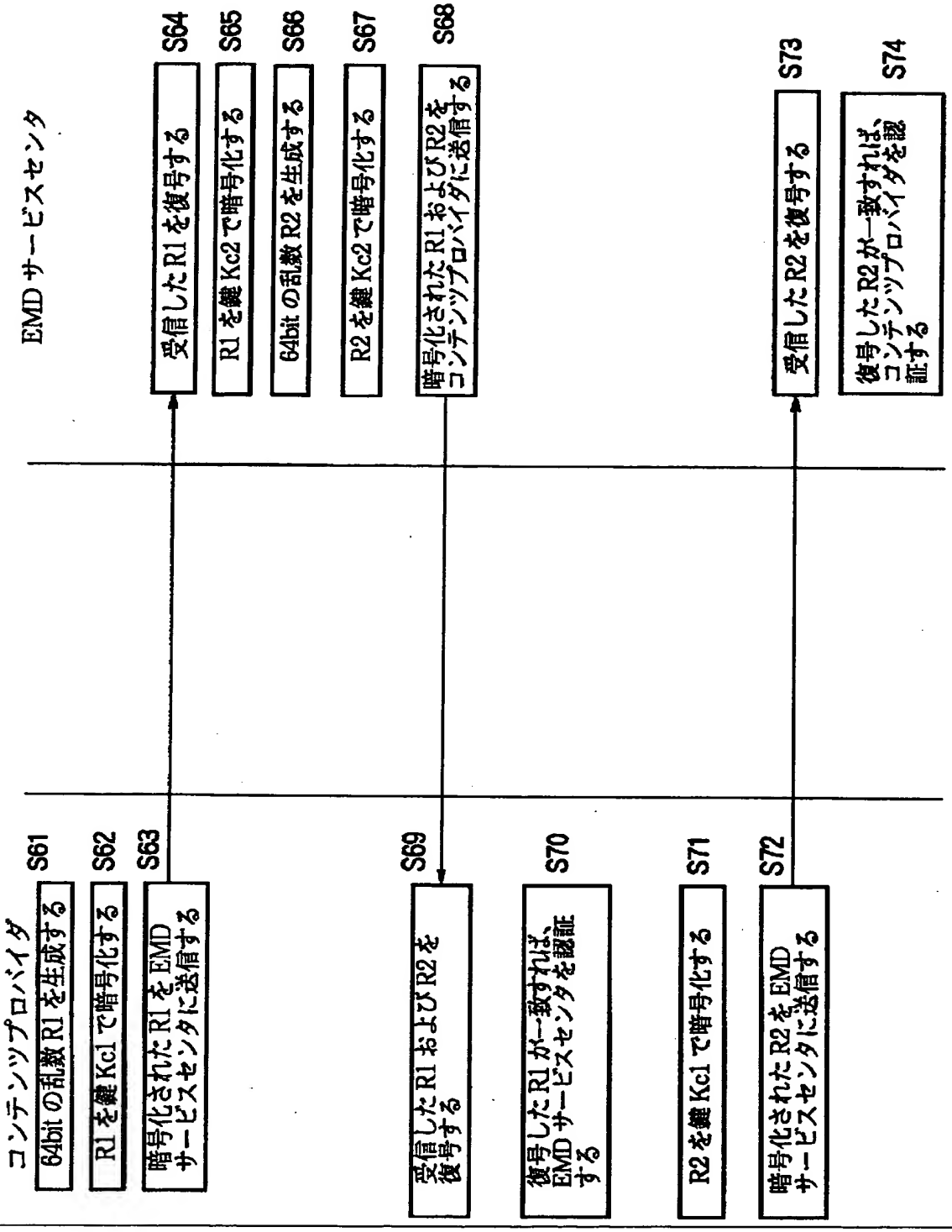
【図３２】


コンテンツプロバイダへの
配送用鍵の送信処理スタート
コンテンツプロバイダと相互認証する
S31
コンテンツプロバイダは配送用鍵を受け取る
S32
コンテンツプロバイダは配送用鍵を記憶する
S33
リターン

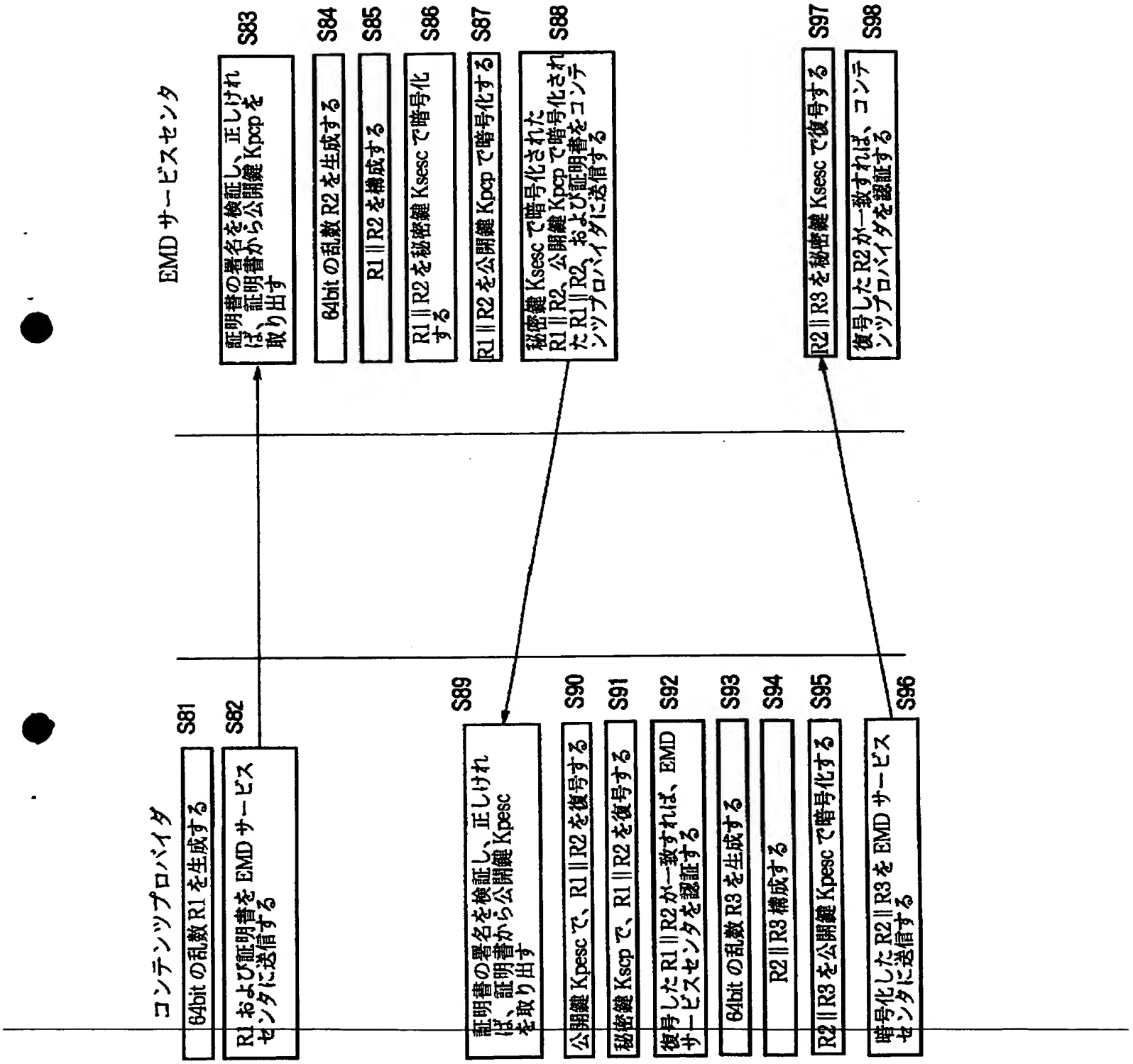
【図３３】


コンテンツプロバイダ
EMDサービスセンタ
S41
64bitの乱数R1を生成する
S42
R1を鍵Kcで暗号化する
S43
暗号化されたR1をEMDサービスセンタに送信する
S44
受信したR1を復号する
S45
32bitの乱数R2を生成する
S46
乱数R1の下位32bitを乱数R2で入れ替え、R1H||R2を得る
S47
R1H||R2を鍵Kcで暗号化する
S48
暗号化されたR1H||R2をコンテンツプロバイダに送信する
S49
受信したR1H||R2を復号する
S50
復号したR1H||R2の上位32bitが一致すれば、EMDサービスセンタを認証する
S51
32bitの乱数R3を生成する
S52
R2||R3を構成する
S53
R2||R3を鍵Kcで暗号化する
S54
暗号化されたR2||R3をEMDサービスセンタに送信する
S55
受信したR2||R3を復号する
S56
復号したR2||R3の上位32bitが一致すれば、コンテンツプロバイダを認証する

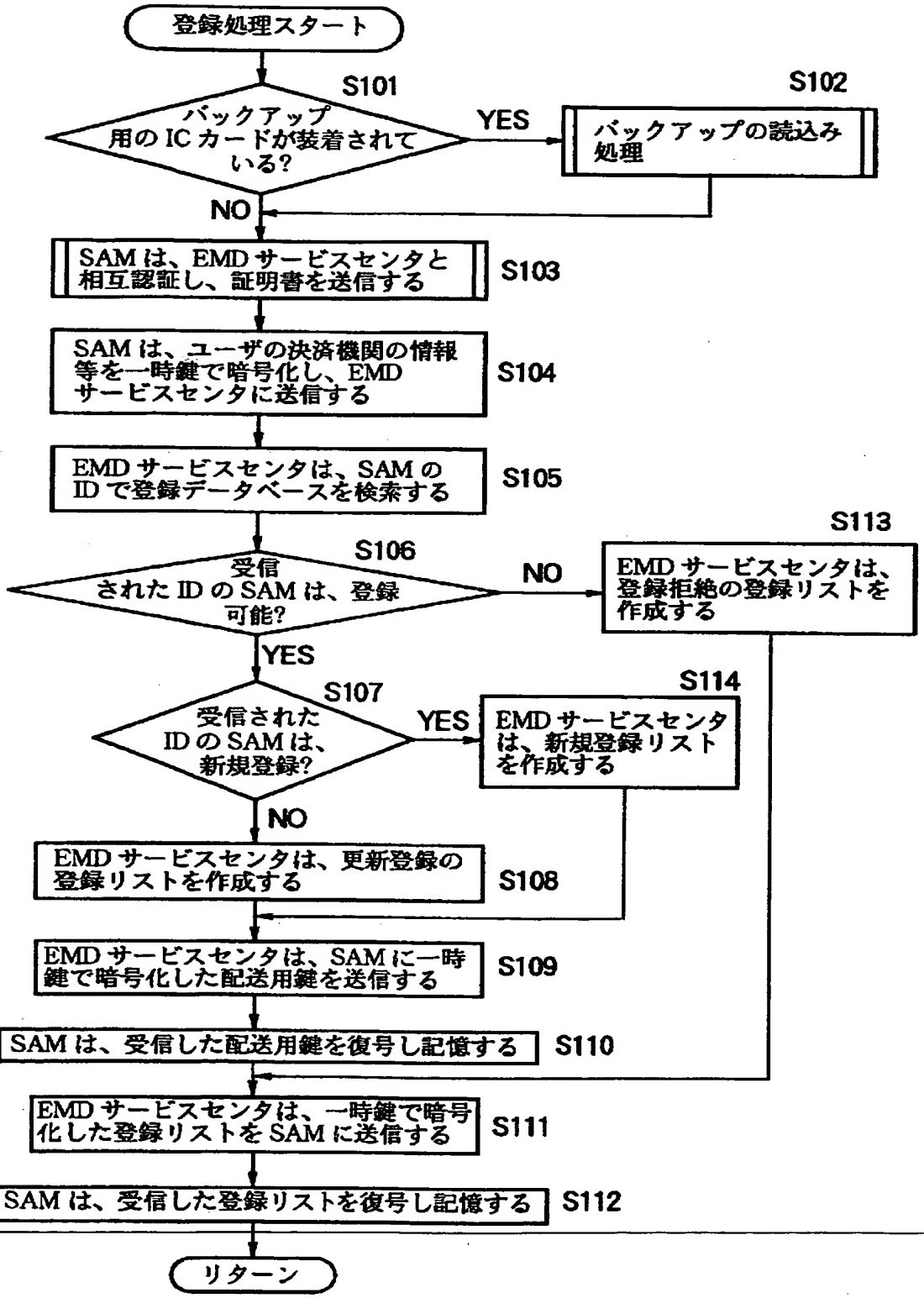
【図３４】


コンテンツプロバイダ
EMDサービスセンタ
S61
64bitの乱数R1を生成する
S62
R1を鍵Kc1で暗号化する
S63
暗号化されたR1をEMDサービスセンタに送信する
S64
受信したR1を復号する
S65
R1を鍵Kc2で暗号化する
S66
64bitの乱数R2を生成する
S67
R2を鍵Kc2で暗号化する
S68
暗号化されたR1およびR2をコンテンツプロバイダに送信する
S69
受信したR1およびR2を復号する
S70
復号したR1が一致すれば、EMDサービスセンタを認証する
S71
R2を鍵Kc1で暗号化する
S72
暗号化されたR2をEMDサービスセンタに送信する
S73
受信したR2を復号する
S74
復号したR2が一致すれば、コンテンツプロバイダを認証する

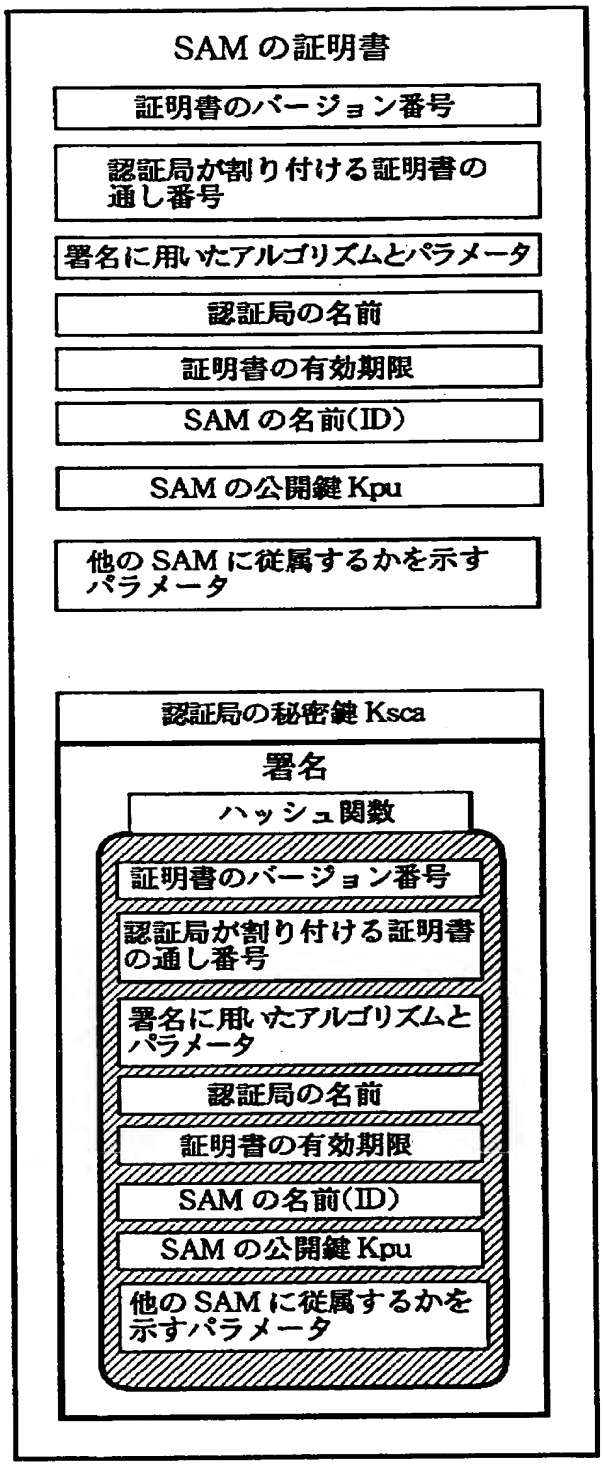
【図３５】


EMDサービスセンタ
コンテンツプロバイダ
S81
64bitの乱数R1を生成する
S82
R1および証明書をEMDサービスセンタに送信する
S83
証明書の署名を検証し、正しければ、証明書から公開鍵Kpcpを取り出す
S84
64bitの乱数R2を生成する
S85
R1‖R2を構成する
S86
R1‖R2を秘密鍵Ksescで暗号化する
S87
R1‖R2を公開鍵Kpcpで暗号化する
S88
秘密鍵Ksescで暗号化されたR1‖R2、公開鍵Kpcpで暗号化されたR1‖R2、および証明書をコンテンツプロバイダに送信する
S89
証明書の署名を検証し、正しければ、証明書から公開鍵Kpescを取り出す
S90
公開鍵Kpescで、R1‖R2を復号する
S91
秘密鍵Kscpで、R1‖R2を復号する
S92
復号したR1‖R2が一致すれば、EMDサービスセンタを認証する
S93
64bitの乱数R3を生成する
S94
R2‖R3構成する
S95
R2‖R3を公開鍵Kpescで暗号化する
S96
暗号化したR2‖R3をEMDサービスセンタに送信する
S97
R2‖R3を秘密鍵Ksescで復号する
S98
復号したR2が一致すれば、コンテンツプロバイダを認証する

【図３６】


登録処理スタート
S101
バックアップ用のICカードが装着されている?
YES
S102
バックアップの読込み処理
NO
SAMは、EMDサービスセンタと相互認証し、証明書を送信する
S103
SAMは、ユーザの決済機関の情報等を一時鍵で暗号化し、EMDサービスセンタに送信する
S104
EMDサービスセンタは、SAMのIDで登録データベースを検索する
S105
S106
受信されたIDのSAMは、登録可能?
NO
S113
EMDサービスセンタは、登録拒絶の登録リストを作成する
YES
S107
受信されたIDのSAMは、新規登録?
YES
S114
EMDサービスセンタは、新規登録リストを作成する
NO
EMDサービスセンタは、更新登録の登録リストを作成する
S108
EMDサービスセンタは、SAMに一時鍵で暗号化した配送用鍵を送信する
S109
SAMは、受信した配送用鍵を復号し記憶する
S110
EMDサービスセンタは、一時鍵で暗号化した登録リストをSAMに送信する
S111
SAMは、受信した登録リストを復号し記憶する
S112
リターン

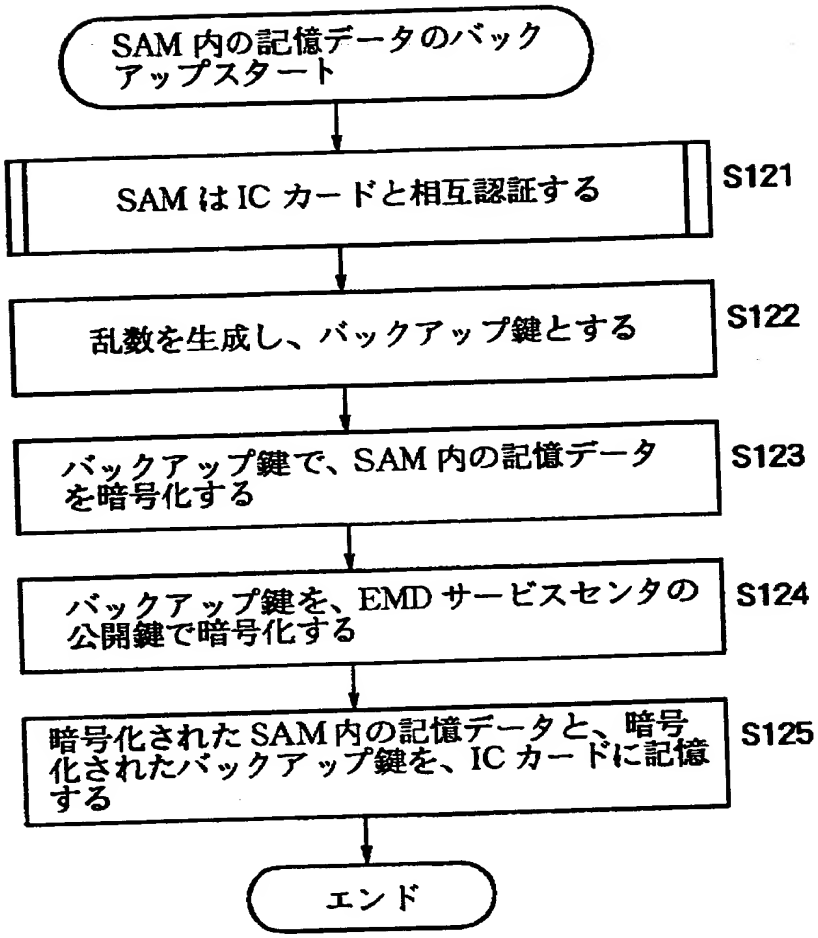
【図３７】


SAMの証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
SAMの名前(ID)
SAMの公開鍵Kpu
他のSAMに従属するかを示すパラメータ
認証局の秘密鍵Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
SAMの名前(ID)
SAMの公開鍵Kpu
他のSAMに従属するかを示すパラメータ

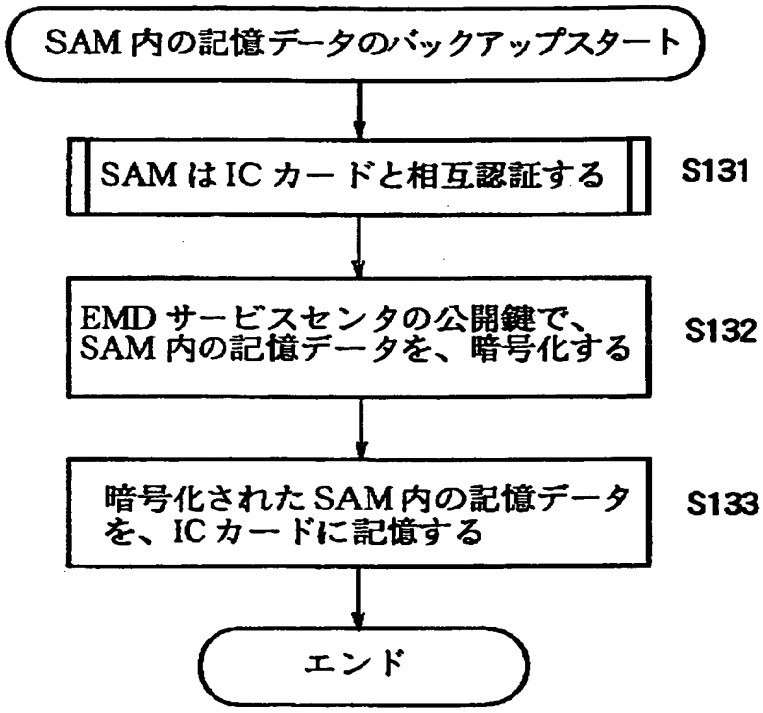
【図３８】

SAMのID (64bit)	登録拒絶フラグ (1bit)	ステータスフラグ (4bit)	コンディションフラグ (1bit)	署名
0000000000000001h	1	0000	0	xxxxxxxxxx
0000000000000002h	1	1010	1	xxxxxxxxxx
0000000000000003h	1	1100	1	xxxxxxxxxx
000000000000000Ah	0	0000	1	xxxxxxxxxx

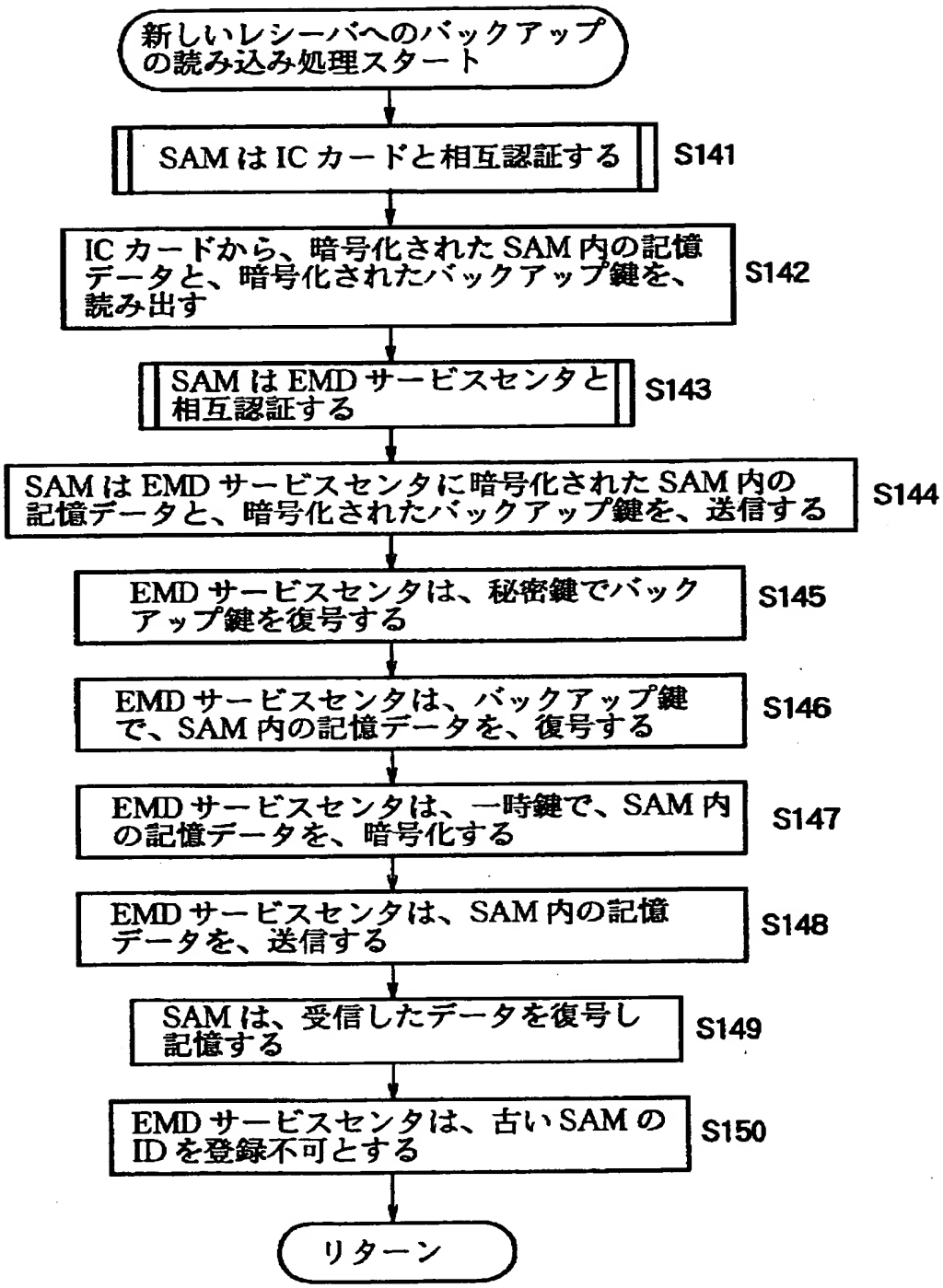
【図３９】


SAM 内の記憶データのバックアップスタート
SAM は IC カードと相互認証する
S121
乱数を生成し、バックアップ鍵とする
S122
バックアップ鍵で、SAM 内の記憶データを暗号化する
S123
バックアップ鍵を、EMD サービスセンタの公開鍵で暗号化する
S124
暗号化された SAM 内の記憶データと、暗号化されたバックアップ鍵を、IC カードに記憶する
S125
エンド

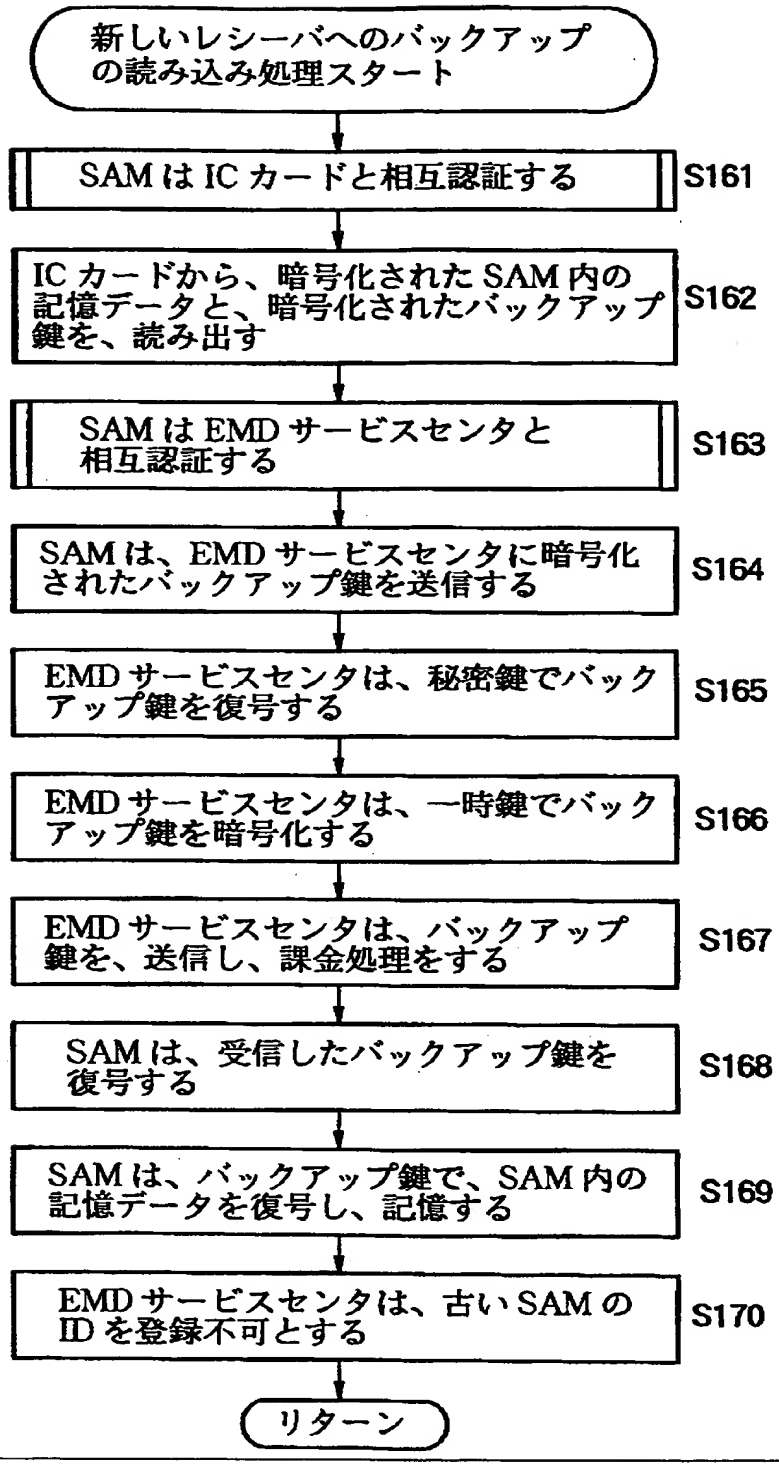
【図４０】


SAM内の記憶データのバックアップスタート
SAMはICカードと相互認証する
S131
EMDサービスセンタの公開鍵で、SAM内の記憶データを、暗号化する
S132
暗号化されたSAM内の記憶データを、ICカードに記憶する
S133
エンド

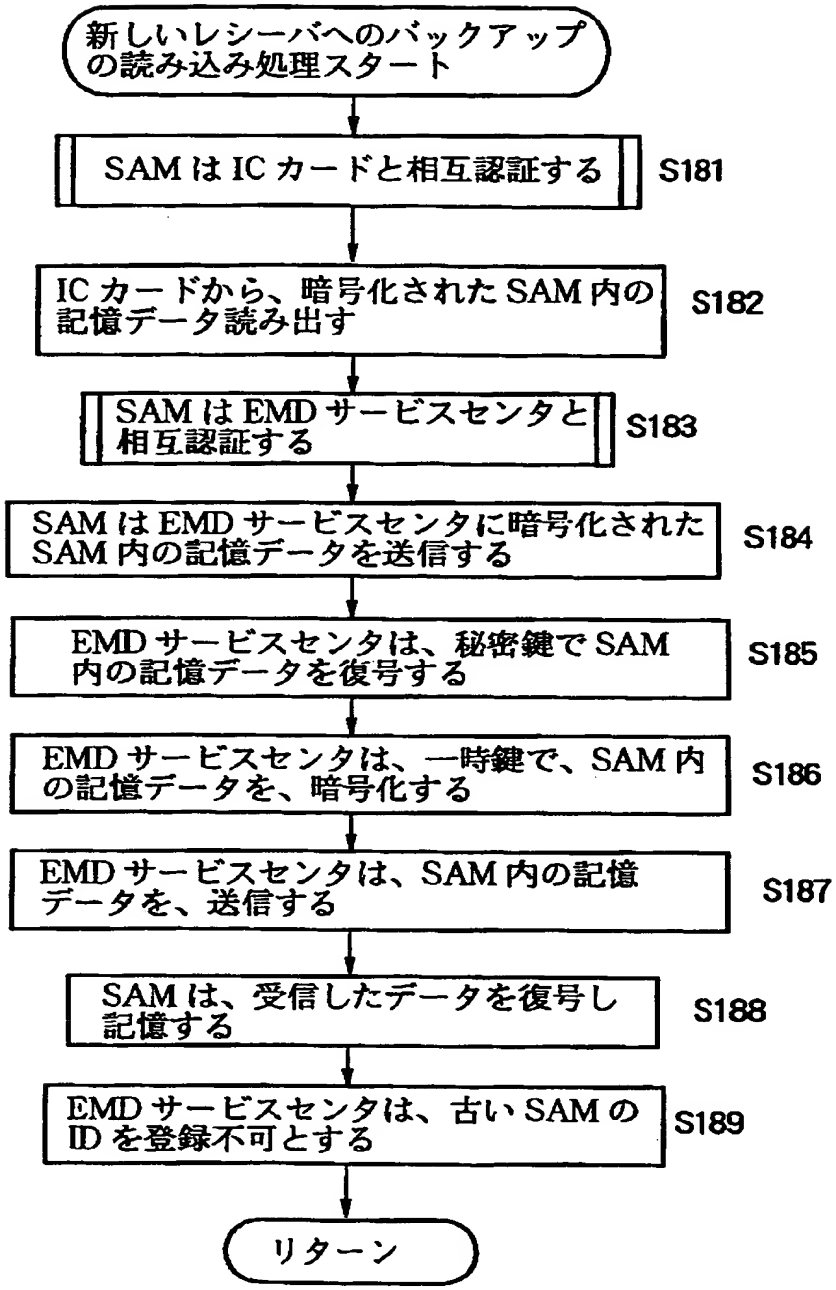
【図４１】


新しいレシーバへのバックアップの読み込み処理スタート
SAMはICカードと相互認証する
S141
ICカードから、暗号化されたSAM内の記憶データと、暗号化されたバックアップ鍵を、読み出す
S142
SAMはEMDサービスセンタと相互認証する
S143
SAMはEMDサービスセンタに暗号化されたSAM内の記憶データと、暗号化されたバックアップ鍵を、送信する
S144
EMDサービスセンタは、秘密鍵でバックアップ鍵を復号する
S145
EMDサービスセンタは、バックアップ鍵で、SAM内の記憶データを、復号する
S146
EMDサービスセンタは、一時鍵で、SAM内の記憶データを、暗号化する
S147
EMDサービスセンタは、SAM内の記憶データを、送信する
S148
SAMは、受信したデータを復号し記憶する
S149
EMDサービスセンタは、古いSAMのIDを登録不可とする
S150
リターン

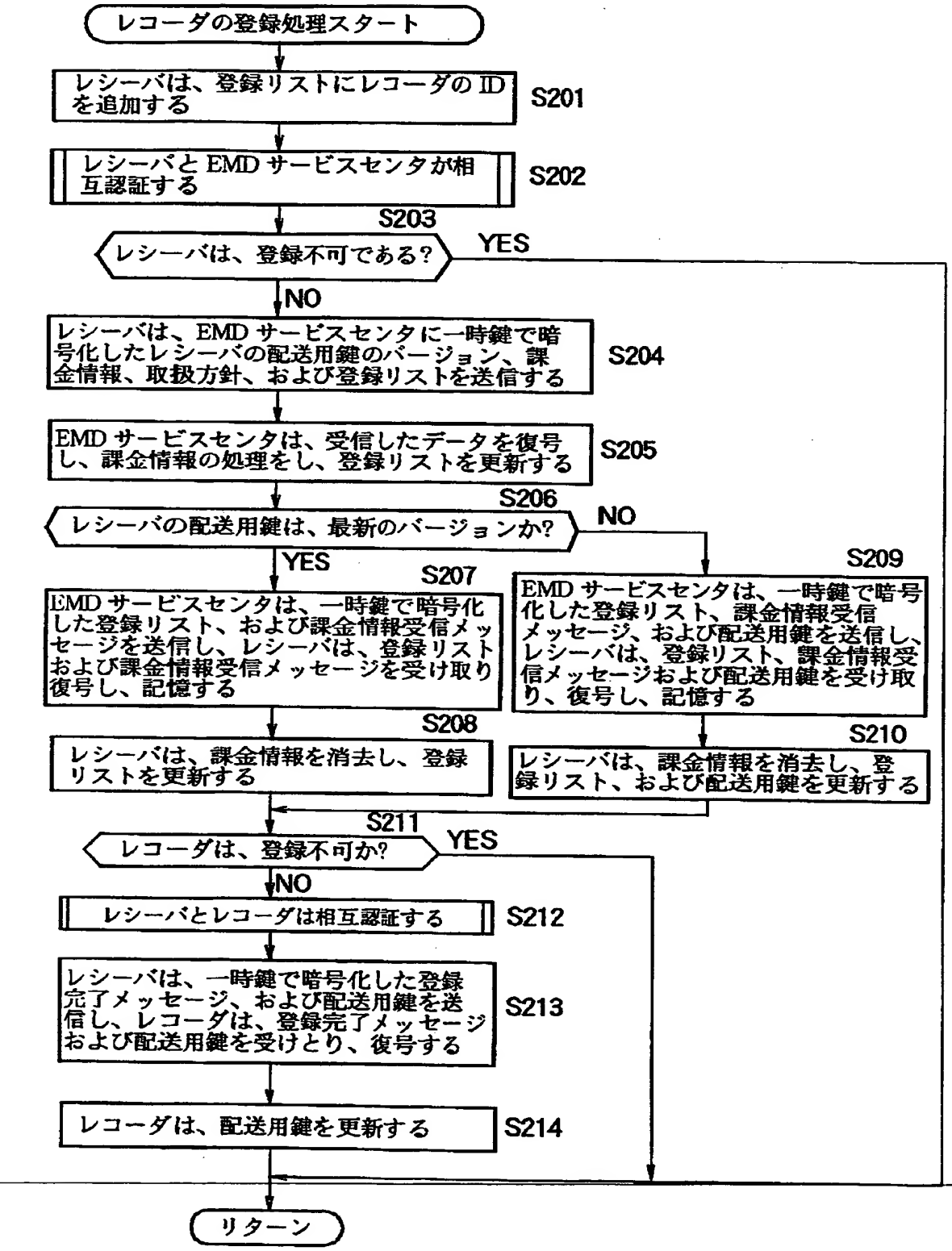
【図４２】


新しいレシーバへのバックアップの読み込み処理スタート
SAMはICカードと相互認証する
S161
ICカードから、暗号化されたSAM内の記憶データと、暗号化されたバックアップ鍵を、読み出す
S162
SAMはEMDサービスセンタと相互認証する
S163
SAMは、EMDサービスセンタに暗号化されたバックアップ鍵を送信する
S164
EMDサービスセンタは、秘密鍵でバックアップ鍵を復号する
S165
EMDサービスセンタは、一時鍵でバックアップ鍵を暗号化する
S166
EMDサービスセンタは、バックアップ鍵を、送信し、課金処理をする
S167
SAMは、受信したバックアップ鍵を復号する
S168
SAMは、バックアップ鍵で、SAM内の記憶データを復号し、記憶する
S169
EMDサービスセンタは、古いSAMのIDを登録不可とする
S170
リターン

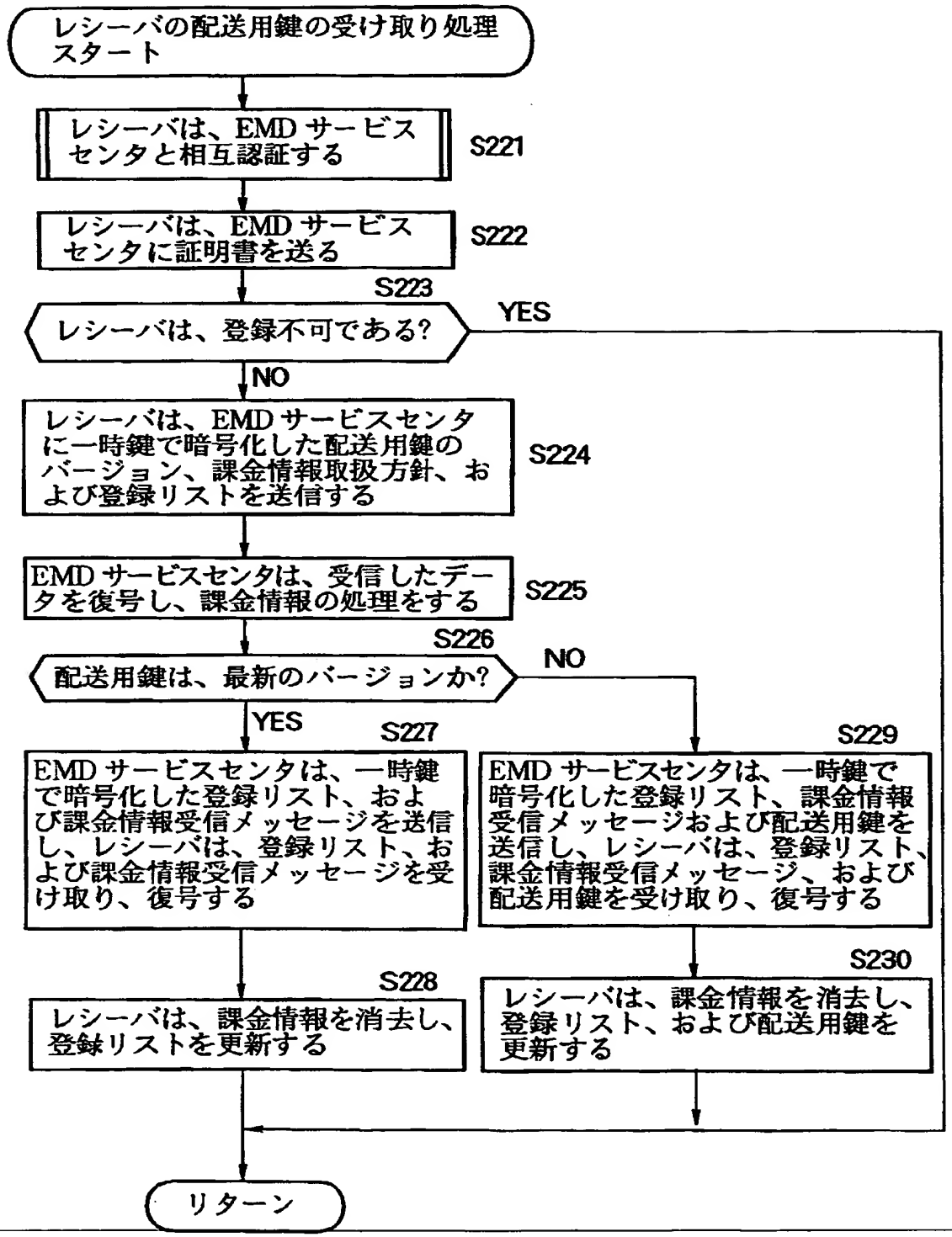
【図４３】


新しいレシーバへのバックアップの読み込み処理スタート
SAMはICカードと相互認証する
S181
ICカードから、暗号化されたSAM内の記憶データ読み出す
S182
SAMはEMDサービスセンタと相互認証する
S183
SAMはEMDサービスセンタに暗号化されたSAM内の記憶データを送信する
S184
EMDサービスセンタは、秘密鍵でSAM内の記憶データを復号する
S185
EMDサービスセンタは、一時鍵で、SAM内の記憶データを、暗号化する
S186
EMDサービスセンタは、SAM内の記憶データを、送信する
S187
SAMは、受信したデータを復号し記憶する
S188
EMDサービスセンタは、古いSAMのIDを登録不可とする
S189
リターン

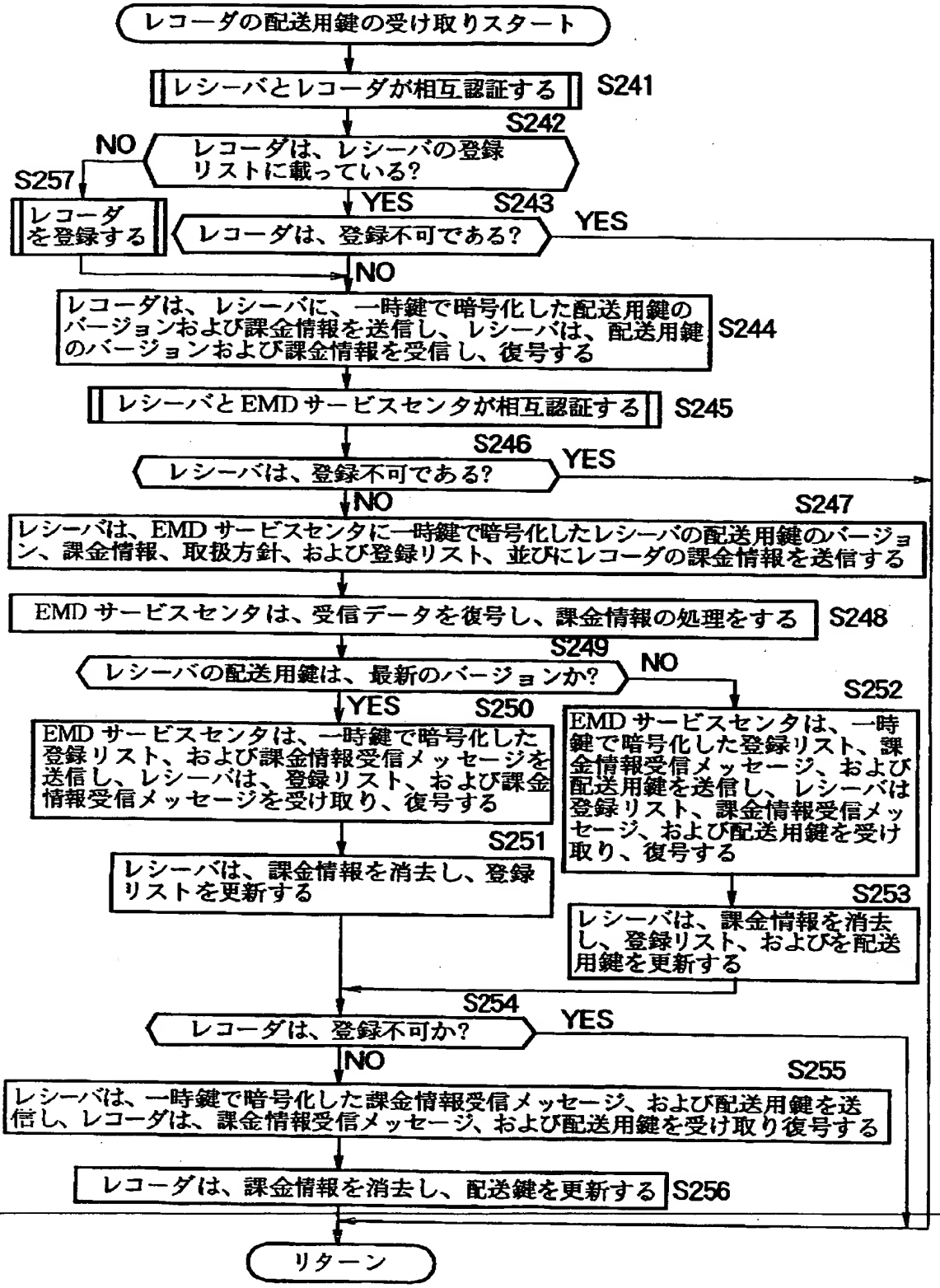
【図４４】


レコーダの登録処理スタート
レシーバは、登録リストにレコーダのIDを追加する
S201
レシーバとEMDサービスセンタが相互認証する
S202
S203
レシーバは、登録不可である?
YES
NO
レシーバは、EMDサービスセンタに一時鍵で暗号化したレシーバの配送用鍵のバージョン、課金情報、取扱方針、および登録リストを送信する
S204
EMDサービスセンタは、受信したデータを復号し、課金情報の処理をし、登録リストを更新する
S205
S206
レシーバの配送用鍵は、最新のバージョンか?
NO
YES
S207
EMDサービスセンタは、一時鍵で暗号化した登録リスト、および課金情報受信メッセージを送信し、レシーバは、登録リストおよび課金情報受信メッセージを受け取り復号し、記憶する
S209
EMDサービスセンタは、一時鍵で暗号化した登録リスト、課金情報受信メッセージ、および配送用鍵を送信し、レシーバは、登録リスト、課金情報受信メッセージおよび配送用鍵を受け取り、復号し、記憶する
S208
レシーバは、課金情報を消去し、登録リストを更新する
S210
レシーバは、課金情報を消去し、登録リスト、および配送用鍵を更新する
S211
レコーダは、登録不可か?
YES
NO
レシーバとレコーダは相互認証する
S212
レシーバは、一時鍵で暗号化した登録完了メッセージ、および配送用鍵を送信し、レコーダは、登録完了メッセージおよび配送用鍵を受けとり、復号する
S213
レコーダは、配送用鍵を更新する
S214
リターン

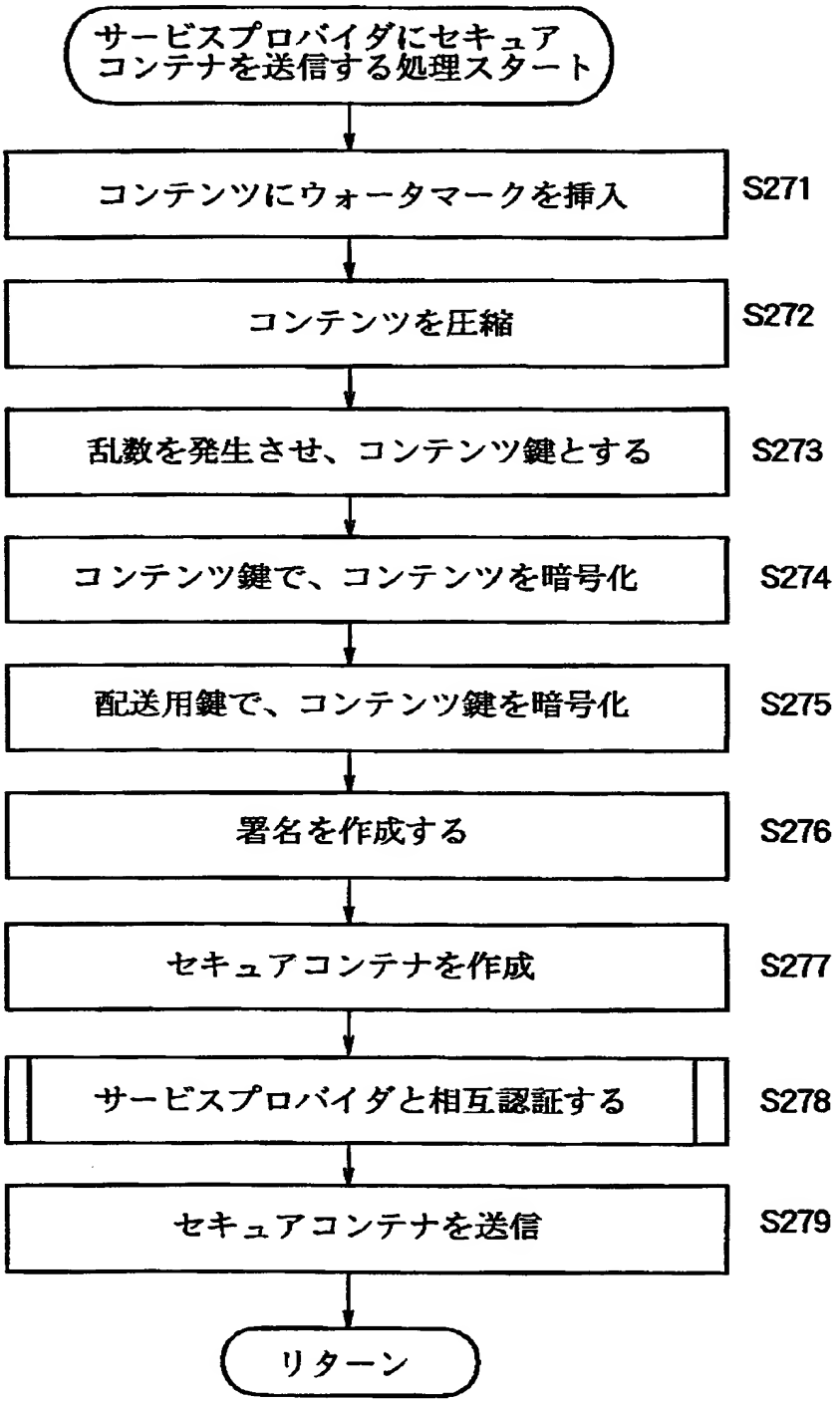
【図４５】


レシーバの配送用鍵の受け取り処理スタート
レシーバは、EMDサービスセンタと相互認証する
S221
レシーバは、EMDサービスセンタに証明書を送る
S222
S223
レシーバは、登録不可である?
YES
NO
レシーバは、EMDサービスセンタに一時鍵で暗号化した配送用鍵のバージョン、課金情報取扱方針、および登録リストを送信する
S224
EMDサービスセンタは、受信したデータを復号し、課金情報の処理をする
S225
S226
配送用鍵は、最新のバージョンか?
NO
YES
S227
EMDサービスセンタは、一時鍵で暗号化した登録リスト、および課金情報受信メッセージを送信し、レシーバは、登録リスト、および課金情報受信メッセージを受け取り、復号する
S229
EMDサービスセンタは、一時鍵で暗号化した登録リスト、課金情報受信メッセージおよび配送用鍵を送信し、レシーバは、登録リスト、課金情報受信メッセージ、および配送用鍵を受け取り、復号する
S230
S228
レシーバは、課金情報を消去し、登録リストを更新する
レシーバは、課金情報を消去し、登録リスト、および配送用鍵を更新する
リターン

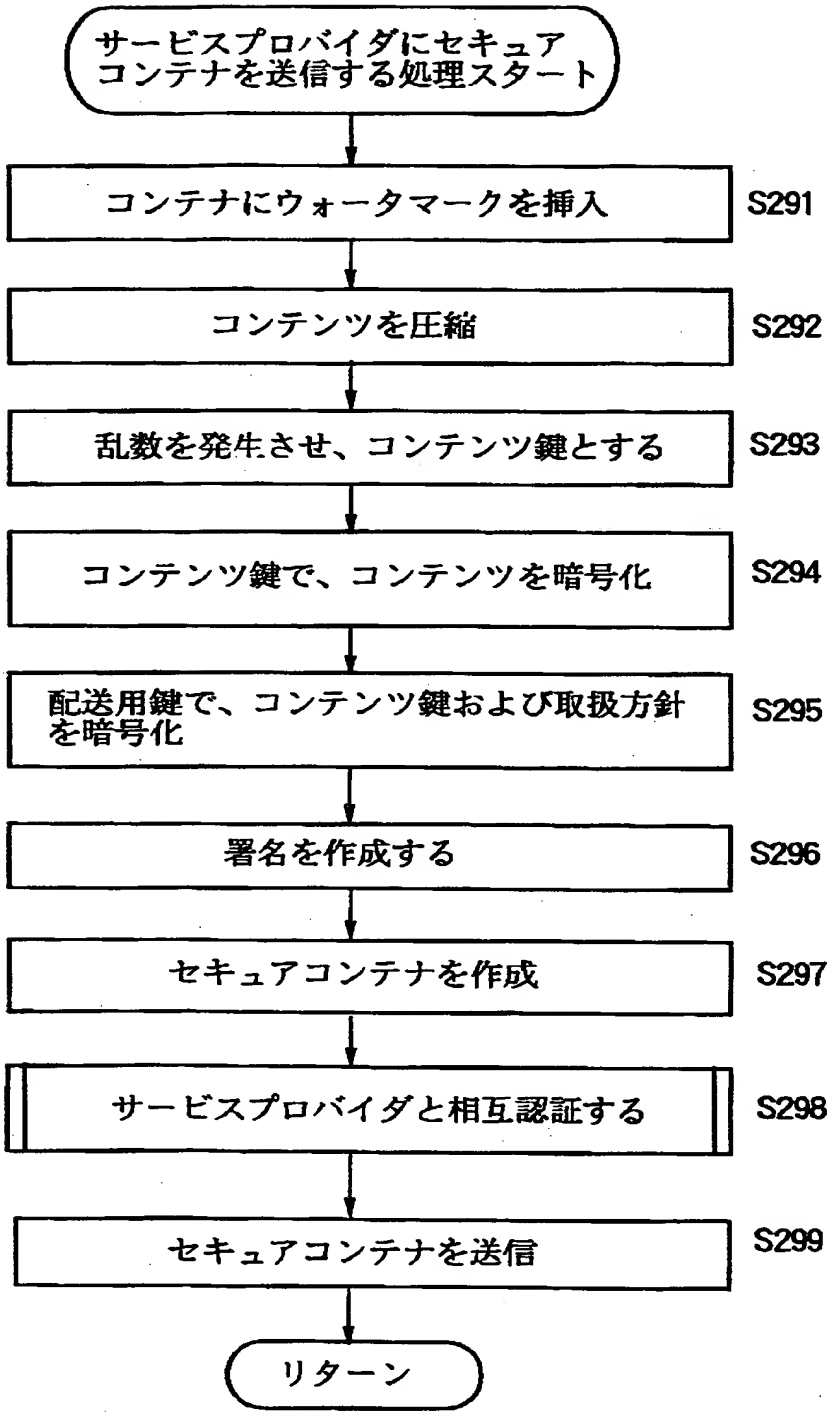
【図４６】


レコーダの配送用鍵の受け取りスタート
レシーバとレコーダが相互認証する
S241
S242
NO
レコーダは、レシーバの登録リストに載っている?
S257
レコーダを登録する
YES
S243
レコーダは、登録不可である?
YES
NO
レコーダは、レシーバに、一時鍵で暗号化した配送用鍵のバージョンおよび課金情報を送信し、レシーバは、配送用鍵のバージョンおよび課金情報を受信し、復号する
S244
レシーバとEMDサービスセンタが相互認証する
S245
S246
レシーバは、登録不可である?
YES
NO
S247
レシーバは、EMDサービスセンタに一時鍵で暗号化したレシーバの配送用鍵のバージョン、課金情報、取扱方針、および登録リスト、並びにレコーダの課金情報を送信する
EMDサービスセンタは、受信データを復号し、課金情報の処理をする
S248
S249
レシーバの配送用鍵は、最新のバージョンか?
NO
YES
S250
EMDサービスセンタは、一時鍵で暗号化した登録リスト、および課金情報受信メッセージを送信し、レシーバは、登録リスト、および課金情報受信メッセージを受け取り、復号する
S252
EMDサービスセンタは、一時鍵で暗号化した登録リスト、課金情報受信メッセージ、および配送用鍵を送信し、レシーバは登録リスト、課金情報受信メッセージ、および配送用鍵を受け取り、復号する
S251
レシーバは、課金情報を消去し、登録リストを更新する
S253
レシーバは、課金情報を消去し、登録リスト、およびを配送用鍵を更新する
S254
レコーダは、登録不可か?
YES
NO
S255
レシーバは、一時鍵で暗号化した課金情報受信メッセージ、および配送用鍵を送信し、レコーダは、課金情報受信メッセージ、および配送用鍵を受け取り復号する
レコーダは、課金情報を消去し、配送鍵を更新する
S256
リターン

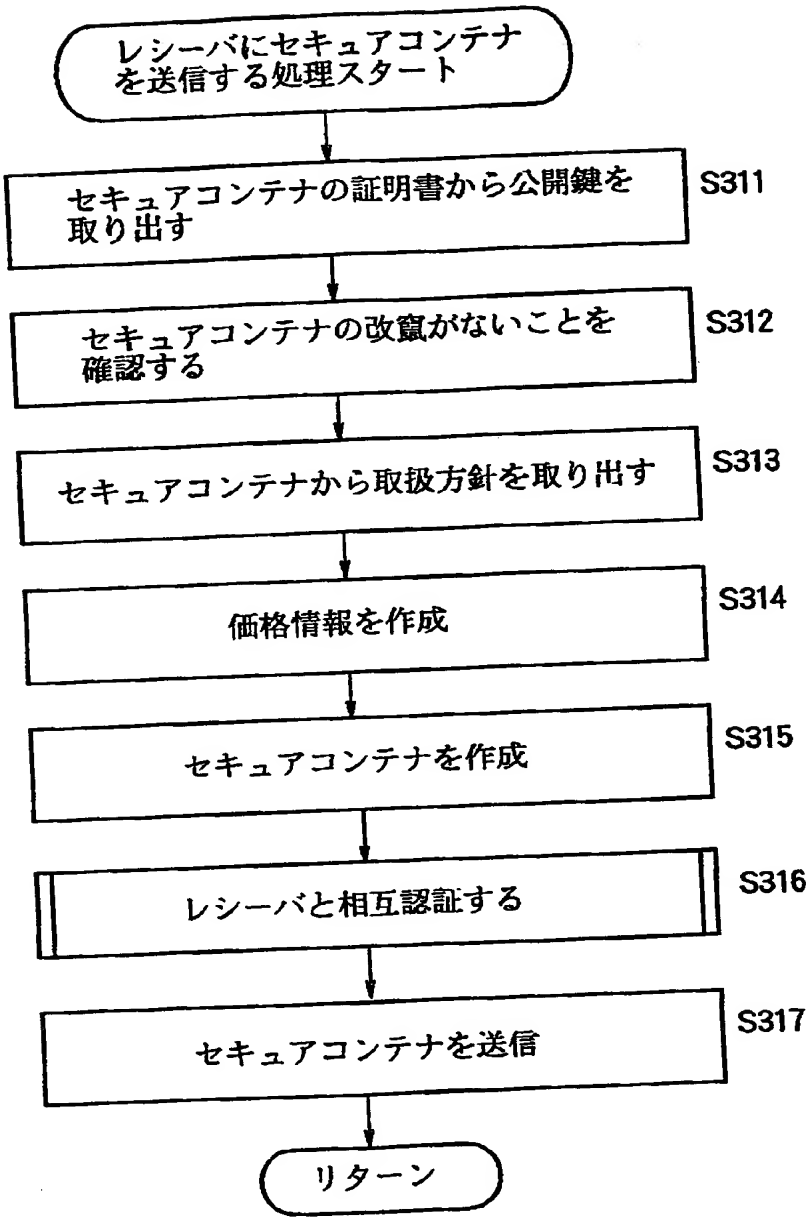
【図４７】


サービスプロバイダにセキュアコンテナを送信する処理スタート
コンテンツにウォータマークを挿入
S271
コンテンツを圧縮
S272
乱数を発生させ、コンテンツ鍵とする
S273
コンテンツ鍵で、コンテンツを暗号化
S274
配送用鍵で、コンテンツ鍵を暗号化
S275
署名を作成する
S276
セキュアコンテナを作成
S277
サービスプロバイダと相互認証する
S278
セキュアコンテナを送信
S279
リターン

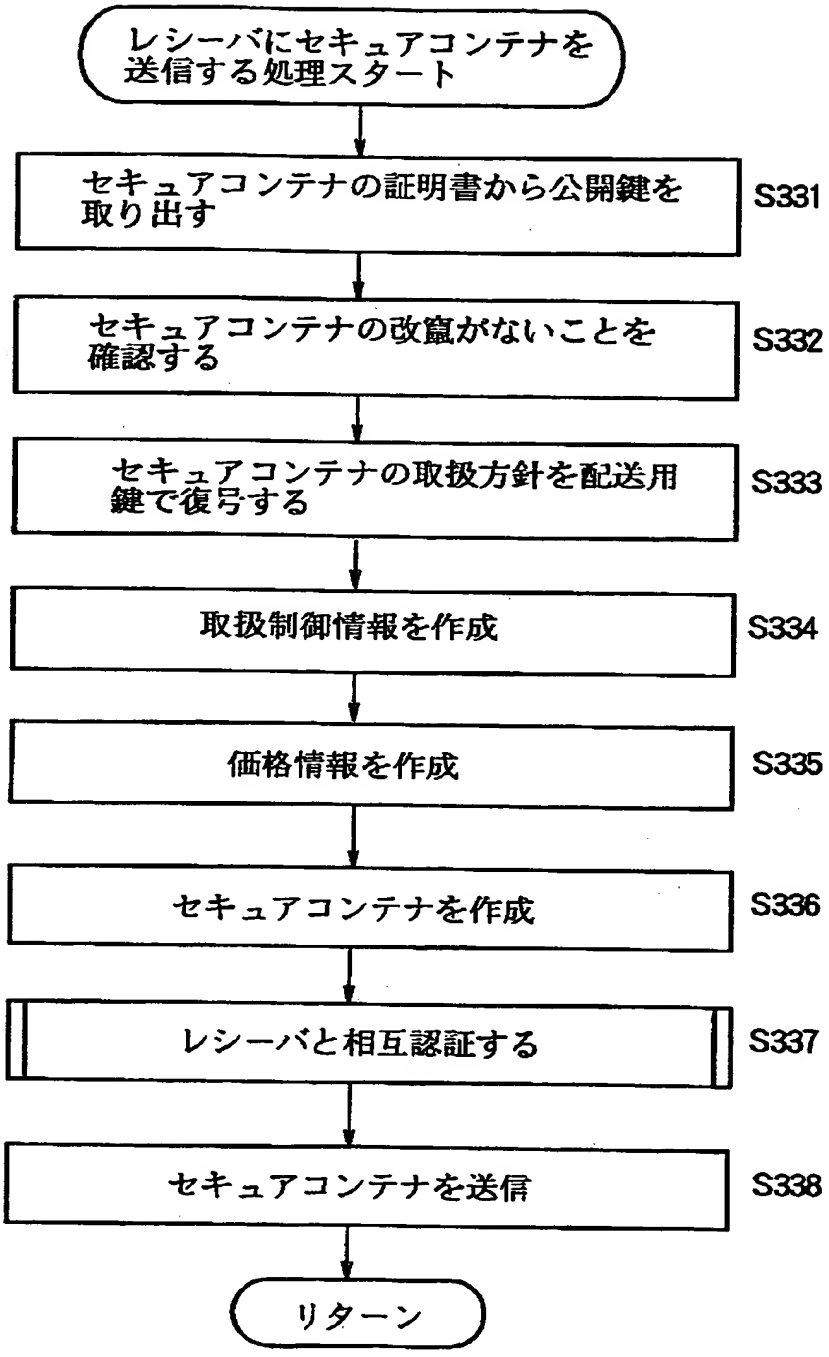
【図４８】


サービスプロバイダにセキュアコンテナを送信する処理スタート
コンテナにウォータマークを挿入
S291
コンテンツを圧縮
S292
乱数を発生させ、コンテンツ鍵とする
S293
コンテンツ鍵で、コンテンツを暗号化
S294
配送用鍵で、コンテンツ鍵および取扱方針を暗号化
S295
署名を作成する
S296
セキュアコンテナを作成
S297
サービスプロバイダと相互認証する
S298
セキュアコンテナを送信
S299
リターン

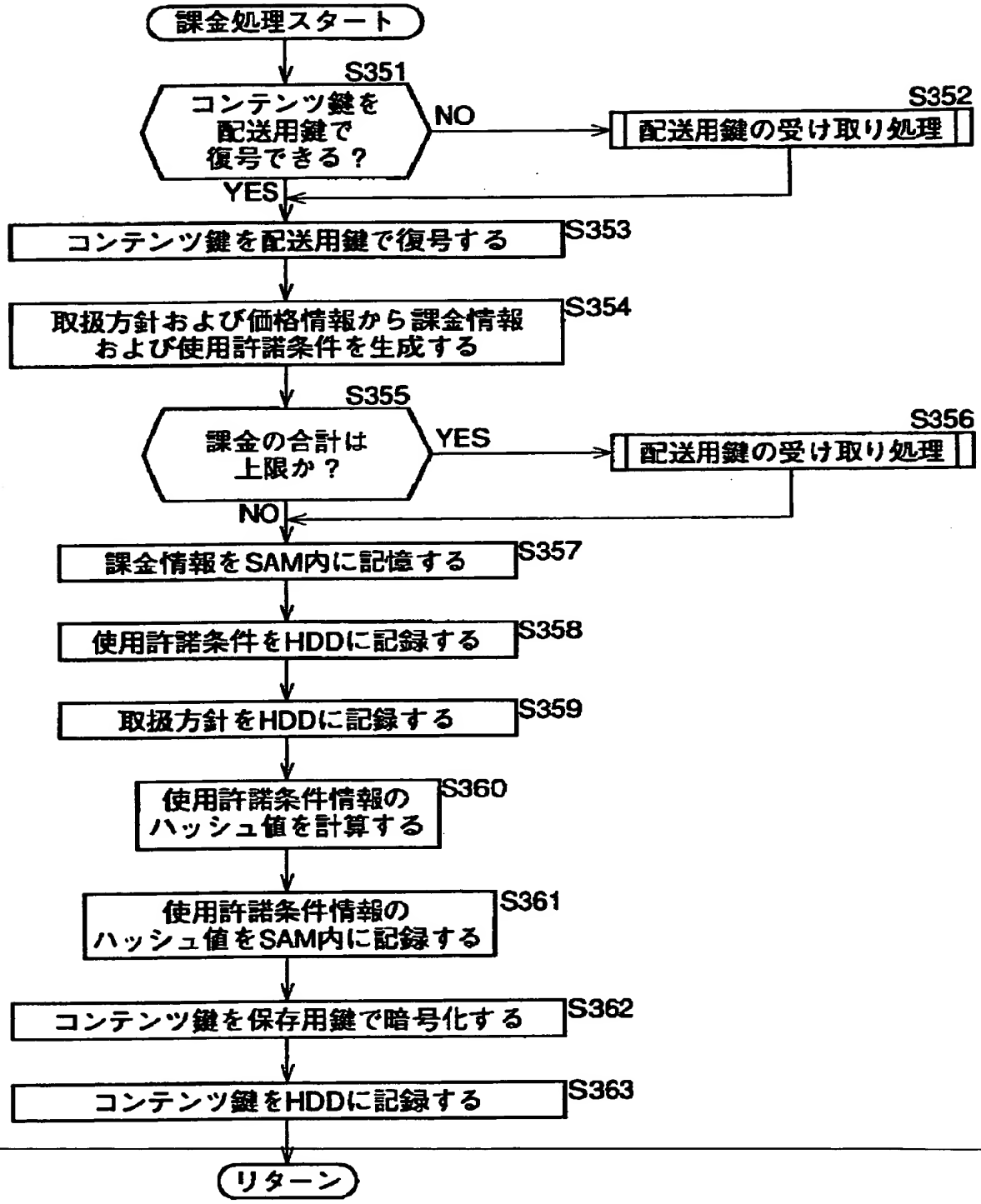
【図４９】


レシーバにセキュアコンテナを送信する処理スタート
セキュアコンテナの証明書から公開鍵を取り出す
S311
セキュアコンテナの改竄がないことを確認する
S312
セキュアコンテナから取扱方針を取り出す
S313
価格情報を作成
S314
セキュアコンテナを作成
S315
レシーバと相互認証する
S316
セキュアコンテナを送信
S317
リターン

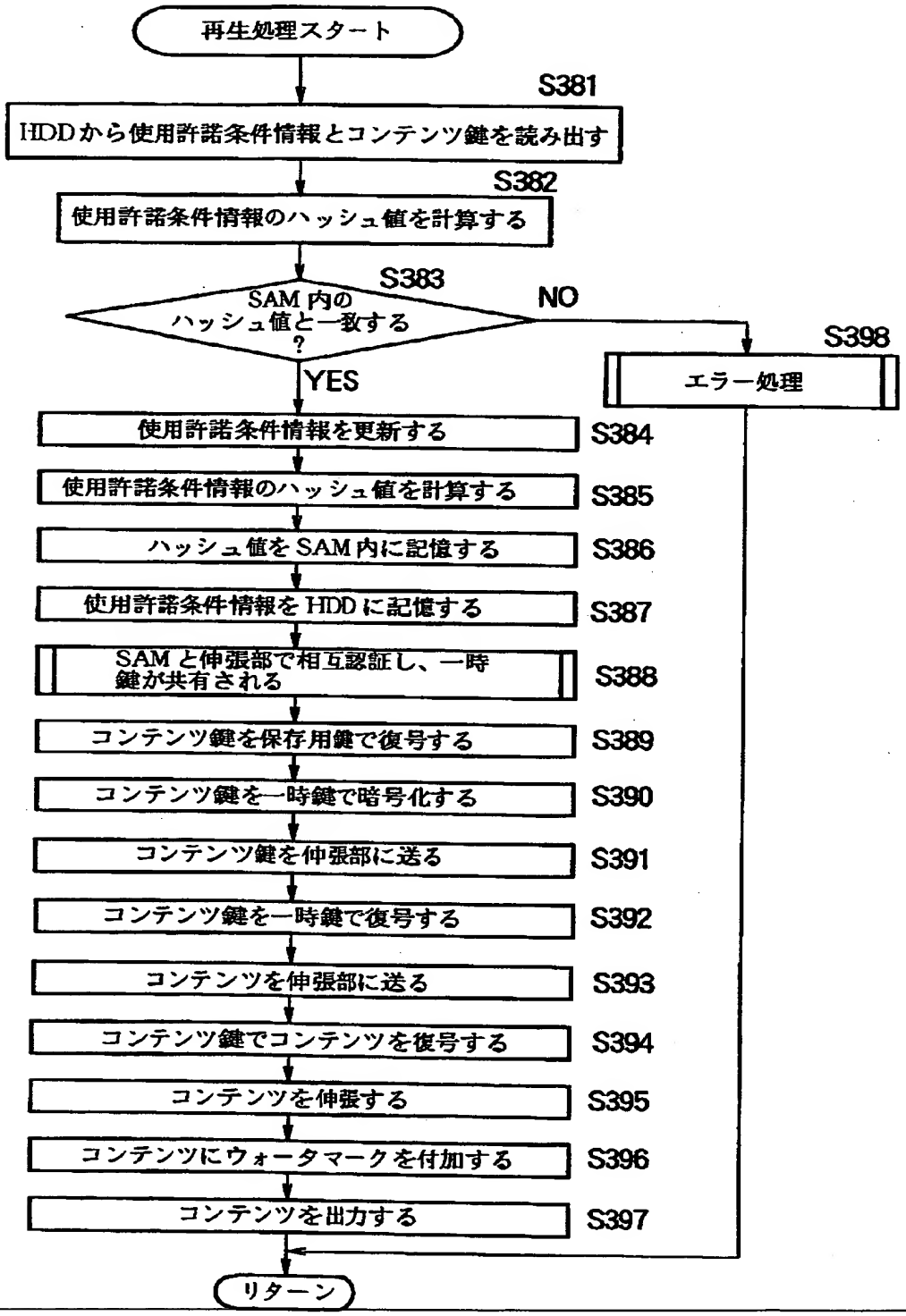
【図５０】


レシーバにセキュアコンテナを送信する処理スタート
セキュアコンテナの証明書から公開鍵を取り出す
S331
セキュアコンテナの改竄がないことを確認する
S332
セキュアコンテナの取扱方針を配送用鍵で復号する
S333
取扱制御情報を作成
S334
価格情報を作成
S335
セキュアコンテナを作成
S336
レシーバと相互認証する
S337
セキュアコンテナを送信
S338
リターン

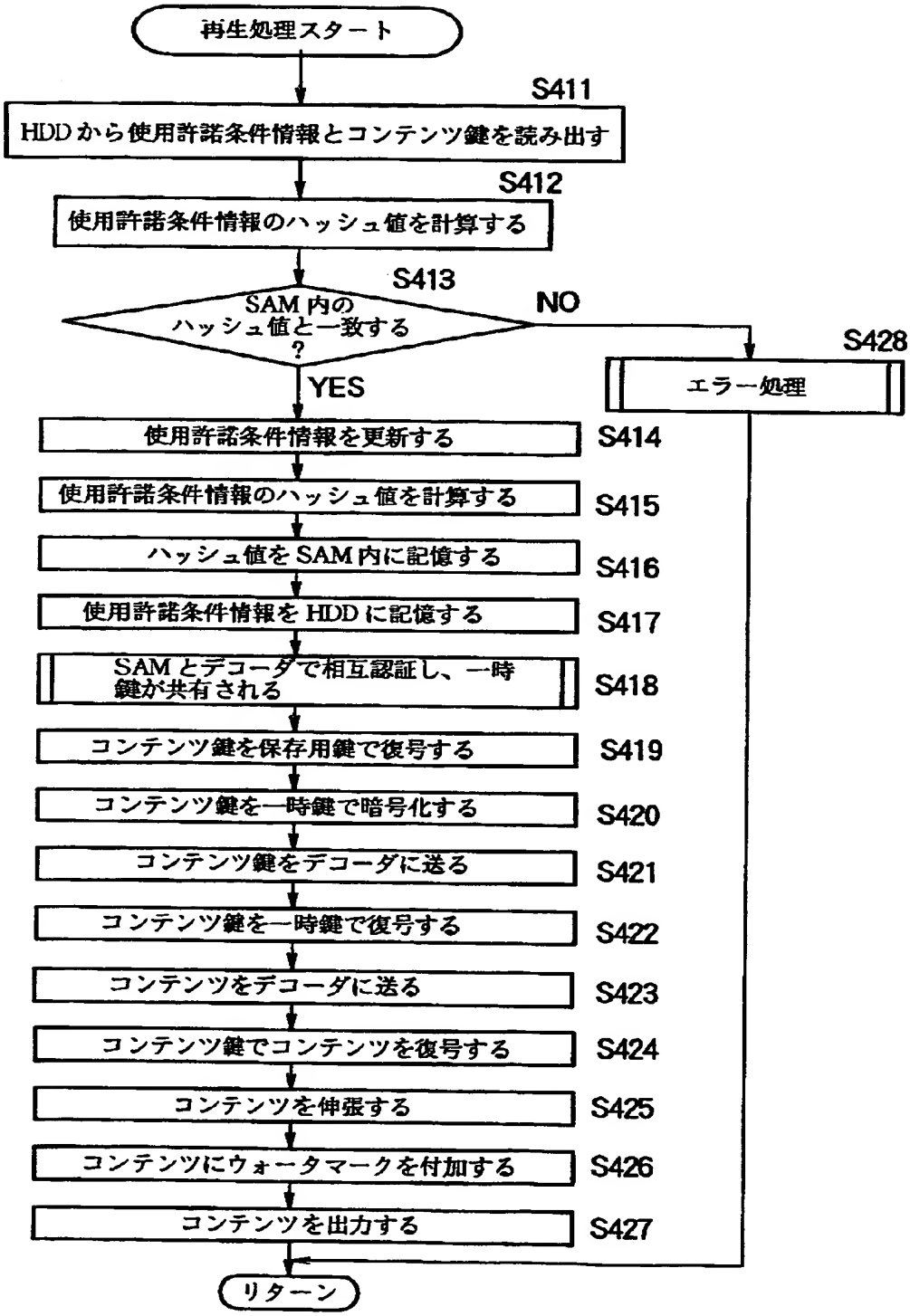
【図５１】


課金処理スタート
S351
コンテンツ鍵を配送用鍵で復号できる？
NO
S352
配送用鍵の受け取り処理
YES
コンテンツ鍵を配送用鍵で復号する
S353
取扱方針および価格情報から課金情報および使用許諾条件を生成する
S354
S355
課金の合計は上限か？
YES
S356
配送用鍵の受け取り処理
NO
課金情報をSAM内に記憶する
S357
使用許諾条件をHDDに記録する
S358
取扱方針をHDDに記録する
S359
使用許諾条件情報のハッシュ値を計算する
S360
使用許諾条件情報のハッシュ値をSAM内に記録する
S361
コンテンツ鍵を保存用鍵で暗号化する
S362
コンテンツ鍵をHDDに記録する
S363
リターン

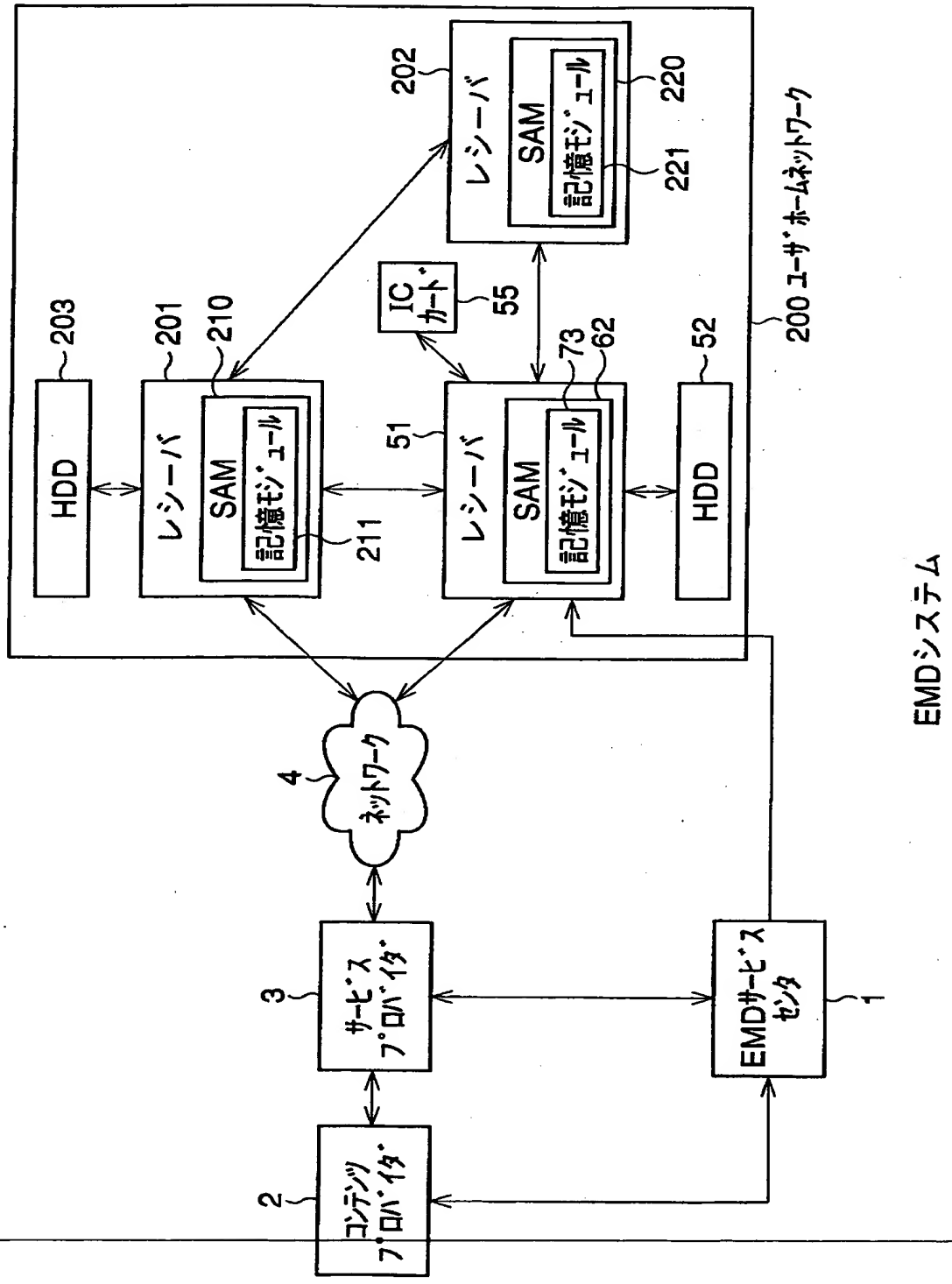
【図５２】


再生処理スタート
S381
HDDから使用許諾条件情報とコンテンツ鍵を読み出す
S382
使用許諾条件情報のハッシュ値を計算する
S383
SAM内のハッシュ値と一致する？
NO
S398
エラー処理
YES
使用許諾条件情報を更新する
S384
使用許諾条件情報のハッシュ値を計算する
S385
ハッシュ値をSAM内に記憶する
S386
使用許諾条件情報をHDDに記憶する
S387
SAMと伸張部で相互認証し、一時鍵が共有される
S388
コンテンツ鍵を保存用鍵で復号する
S389
コンテンツ鍵を一時鍵で暗号化する
S390
コンテンツ鍵を伸張部に送る
S391
コンテンツ鍵を一時鍵で復号する
S392
コンテンツを伸張部に送る
S393
コンテンツ鍵でコンテンツを復号する
S394
コンテンツを伸張する
S395
コンテンツにウォータマークを付加する
S396
コンテンツを出力する
S397
リターン

【図５３】


再生処理スタート
S411
HDDから使用許諾条件情報とコンテンツ鍵を読み出す
S412
使用許諾条件情報のハッシュ値を計算する
S413
SAM内のハッシュ値と一致する？
NO
S428
エラー処理
YES
使用許諾条件情報を更新する
S414
使用許諾条件情報のハッシュ値を計算する
S415
ハッシュ値をSAM内に記憶する
S416
使用許諾条件情報をHDDに記憶する
S417
SAMとデコーダで相互認証し、一時鍵が共有される
S418
コンテンツ鍵を保存用鍵で復号する
S419
コンテンツ鍵を一時鍵で暗号化する
S420
コンテンツ鍵をデコーダに送る
S421
コンテンツ鍵を一時鍵で復号する
S422
コンテンツをデコーダに送る
S423
コンテンツ鍵でコンテンツを復号する
S424
コンテンツを伸張する
S425
コンテンツにウォータマークを付加する
S426
コンテンツを出力する
S427
リターン

【図54】


EMDシステム
200 ユーザ・ホームネットワーク
202
レシーバ
SAM
記憶モジュール
220
221
IC カード
55
203
201
210
HDD
レシーバ
SAM
記憶モジュール
211
51
レシーバ
SAM
記憶モジュール
73
62
52
HDD
4
ネットワーク
3
サービス プロバイダ
EMDサービス センタ
1
2
コンテンツ プロバイダ

【図55】

リスト部

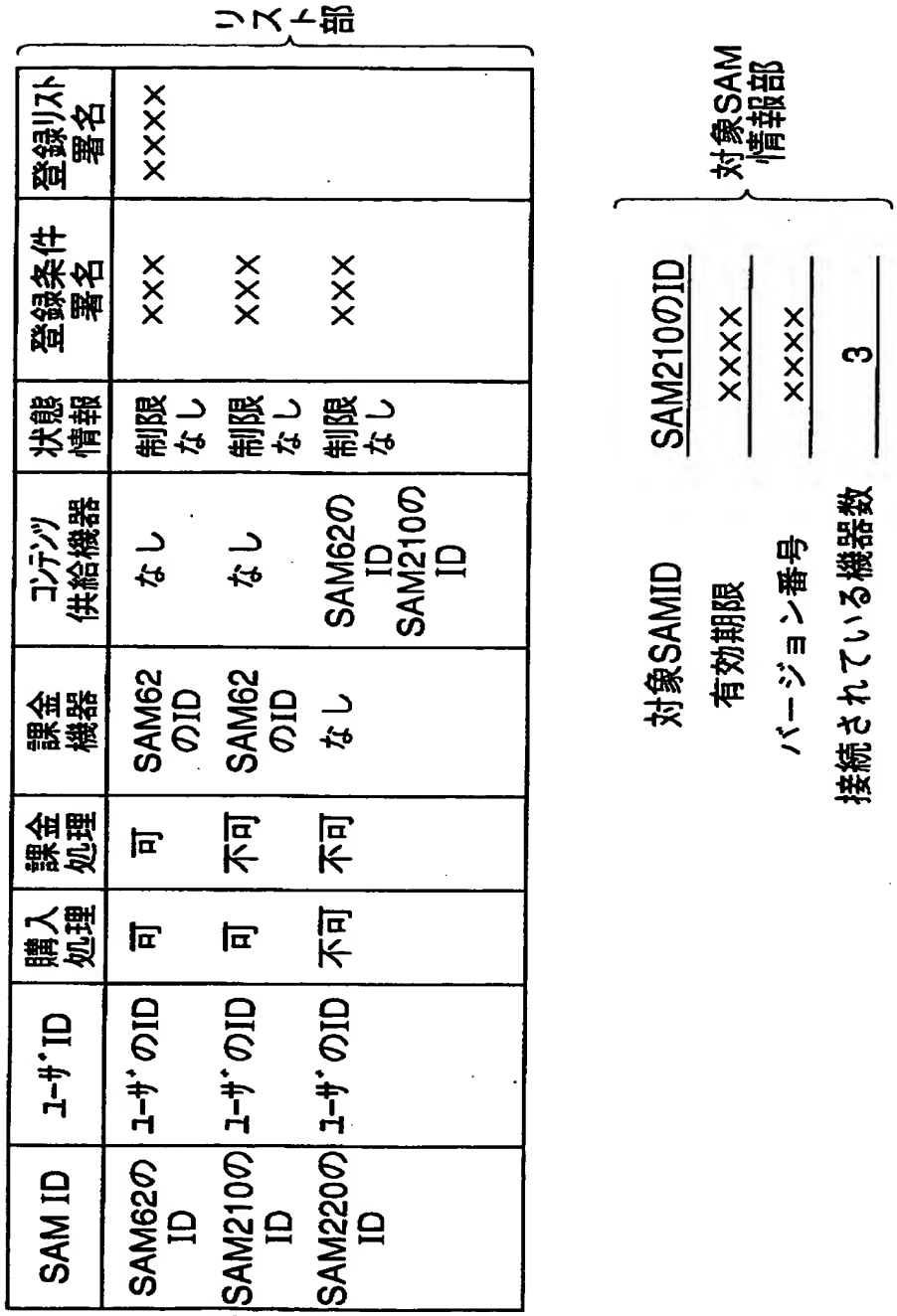
	SAM ID	ユーザID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態情報	登録条件署名	登録リスト署名
レシーバ51の登録条件	SAM62のID	ユーザのID	可	可	SAM62のID	なし	制限なし	×××	××××
レシーバ201の登録条件	SAM210のID	ユーザのID	可	不可	SAM62のID	なし	制限なし	×××	
レシーバ202の登録条件	SAM220のID	ユーザのID	不可	不可	なし	SAM62のID SAM210のID	制限なし	×××	

対象SAM情報部

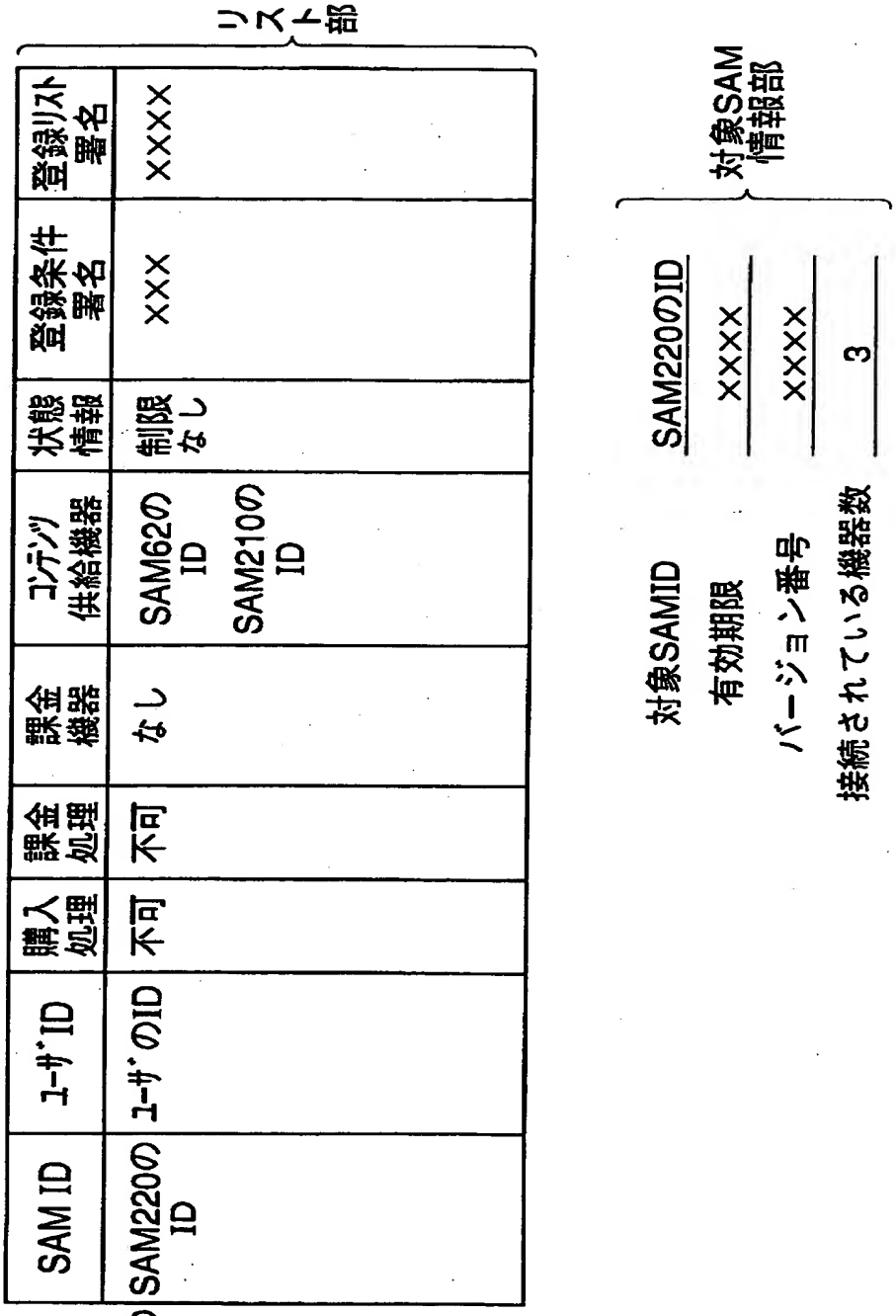
対象SAMID	SAM62のID
有効期限	××××
バージョン番号	××××
接続されている機器数	3

レシーバ51の登録リスト

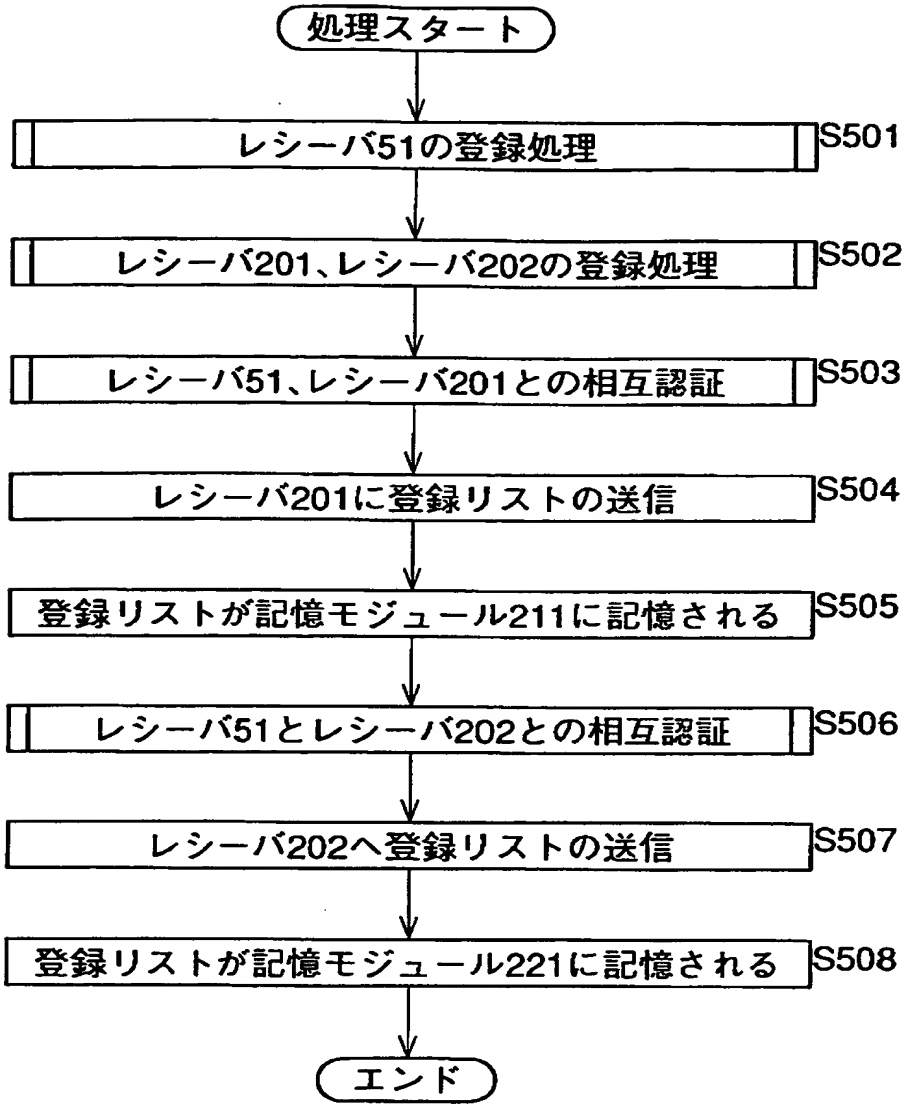
【図56】


リスト部
SAM ID
ユーザ'ID
購入処理
課金処理
課金機器
コンテンツ供給機器
状態情報
登録条件署名
登録リスト署名
レシーバ'51の登録条件
SAM62のID
ユーザ'のID
可
可
SAM62のID
なし
制限なし
×××
××××
レシーバ'201の登録条件
SAM210のID
ユーザ'のID
可
不可
SAM62のID
なし
制限なし
×××
レシーバ'202の登録条件
SAM220のID
ユーザ'のID
不可
不可
なし
SAM62のID SAM210のID
制限なし
×××
対象SAM情報部
対象SAMID
SAM210のID
有効期限
××××
バージョン番号
××××
接続されている機器数
3
レシーバ201の登録リスト

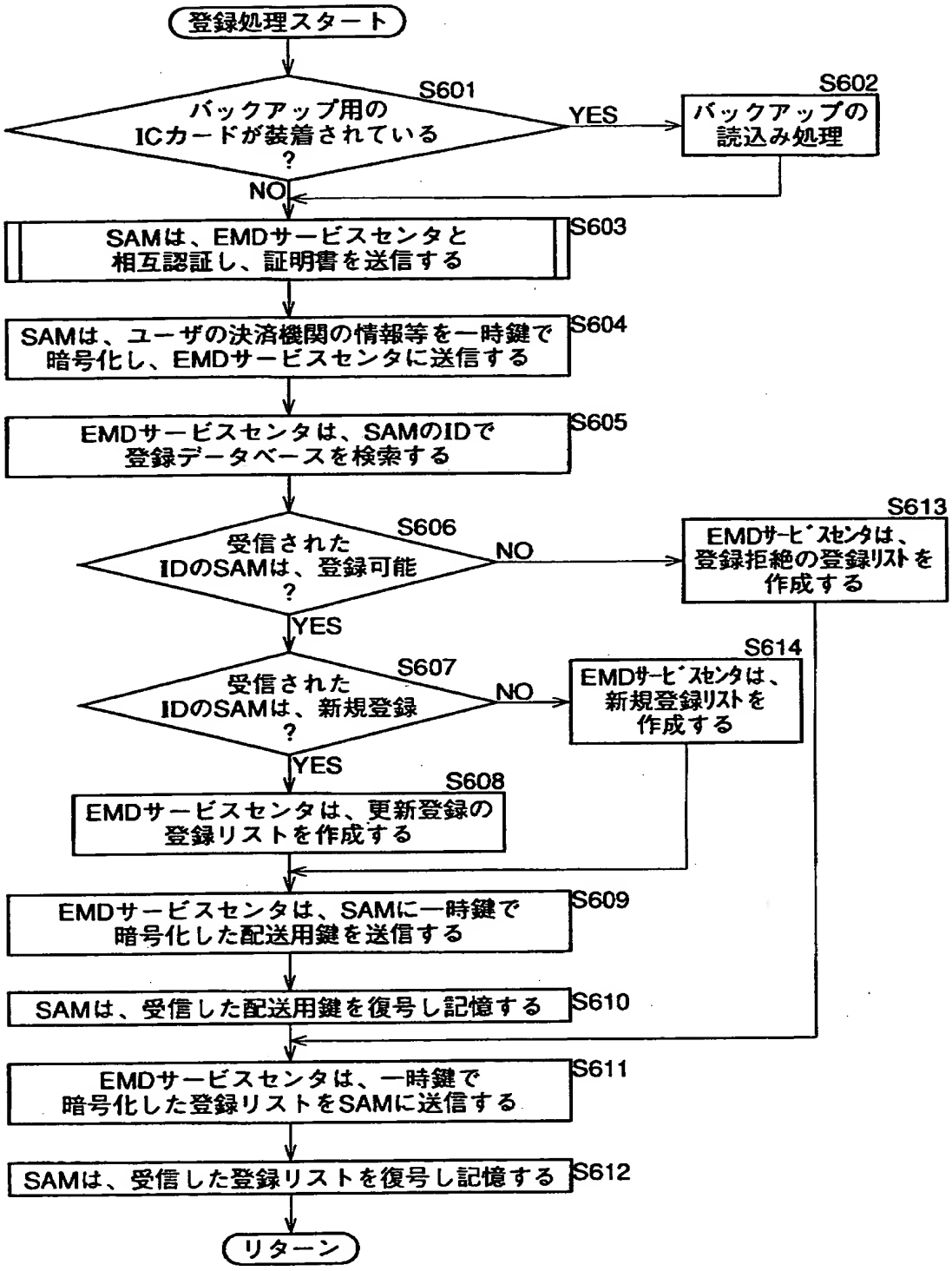
【図57】


リスト部
SAM ID
ユーザID
購入処理
課金処理
課金機器
コンテンツ供給機器
状態情報
登録条件署名
登録リスト署名
レシーバ202の登録条件
SAM220のID
ユーザのID
不可
不可
なし
SAM62のID
SAM210のID
制限なし
XXX
XXXX
対象SAM情報部
対象SAMID
SAM220のID
有効期限
XXXX
バージョン番号
XXXX
接続されている機器数
3
レシーバ202の登録リスト

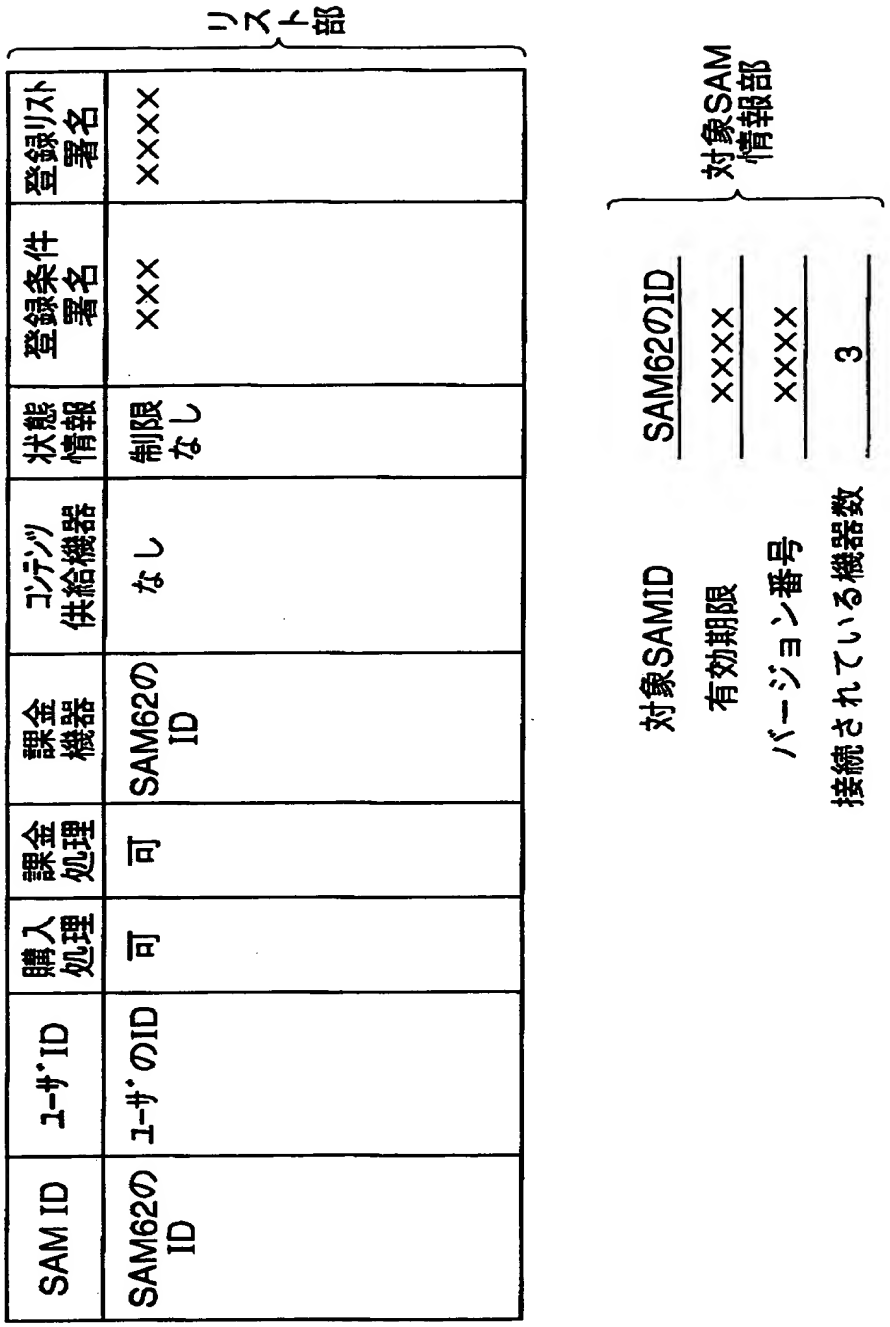
【図58】


処理スタート
レシーバ51の登録処理
S501
レシーバ201、レシーバ202の登録処理
S502
レシーバ51、レシーバ201との相互認証
S503
レシーバ201に登録リストの送信
S504
登録リストが記憶モジュール211に記憶される
S505
レシーバ51とレシーバ202との相互認証
S506
レシーバ202へ登録リストの送信
S507
登録リストが記憶モジュール221に記憶される
S508
エンド

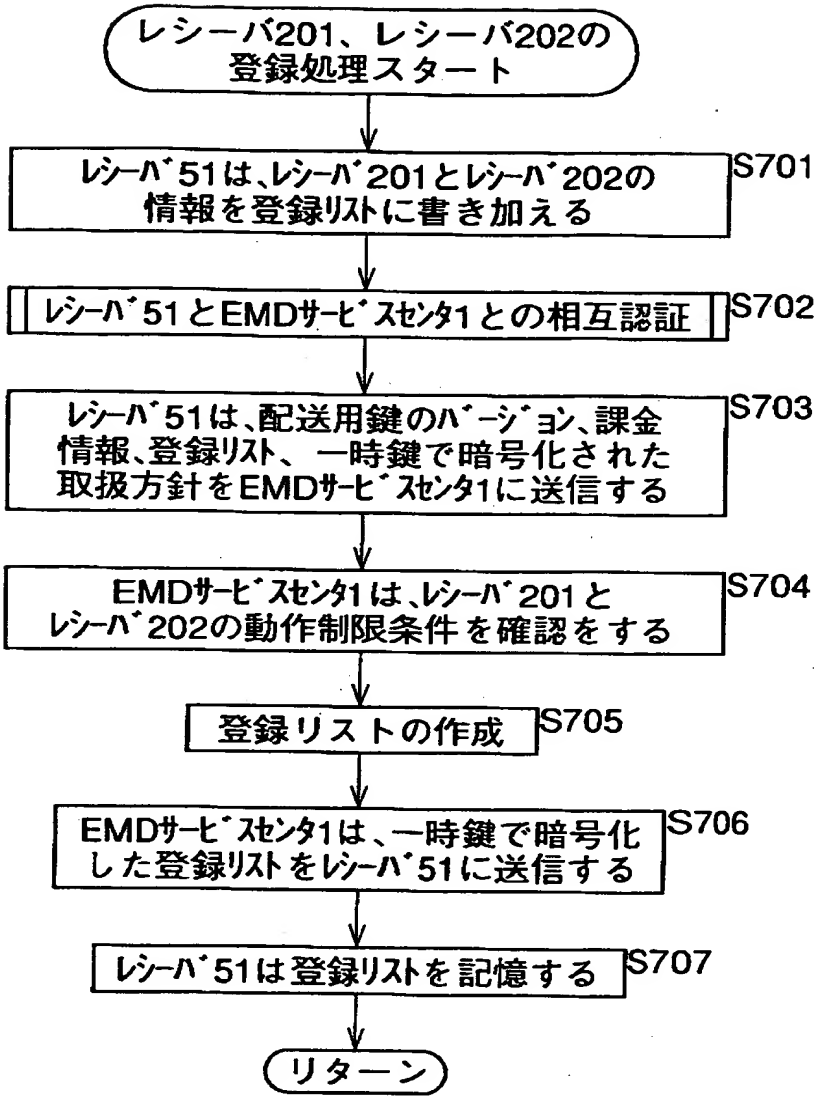
【図59】


登録処理スタート
S601
バックアップ用の
ICカードが装着されている
？
YES
S602
バックアップの
読込み処理
NO
SAMは、EMDサービスセンタと
相互認証し、証明書を送信する
S603
SAMは、ユーザの決済機関の情報等を一時鍵で
暗号化し、EMDサービスセンタに送信する
S604
EMDサービスセンタは、SAMのIDで
登録データベースを検索する
S605
S606
受信された
IDのSAMは、登録可能
？
NO
S613
EMDｻｰﾋﾞｽｾﾝﾀは、
登録拒絶の登録ﾘｽﾄを
作成する
YES
S607
受信された
IDのSAMは、新規登録
？
NO
S614
EMDｻｰﾋﾞｽｾﾝﾀは、
新規登録ﾘｽﾄを
作成する
YES
S608
EMDサービスセンタは、更新登録の
登録リストを作成する
EMDサービスセンタは、SAMに一時鍵で
暗号化した配送用鍵を送信する
S609
SAMは、受信した配送用鍵を復号し記憶する
S610
EMDサービスセンタは、一時鍵で
暗号化した登録リストをSAMに送信する
S611
SAMは、受信した登録リストを復号し記憶する
S612
リターン

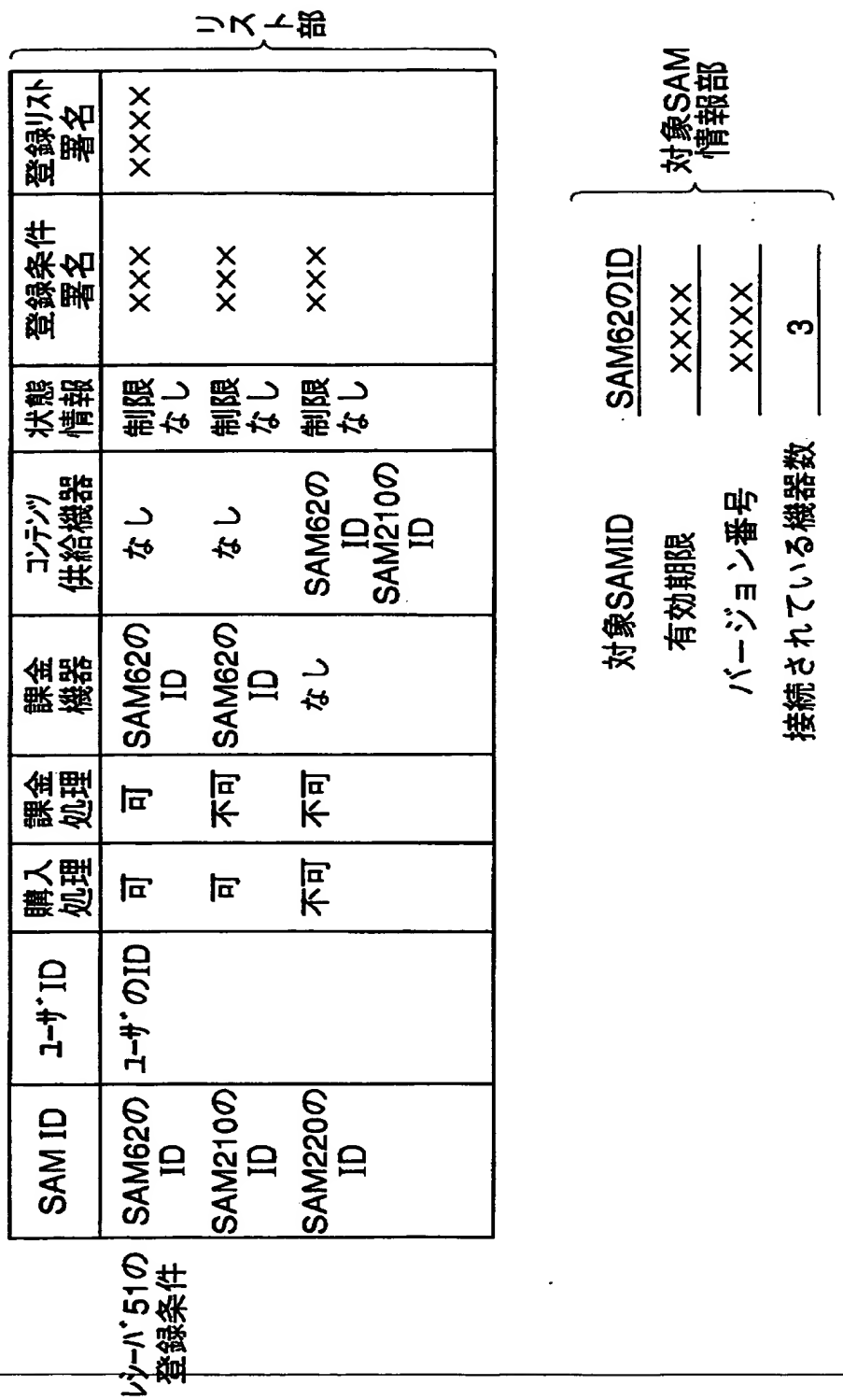
【図60】


リスト部
SAM ID
ユーザID
購入処理
課金処理
課金機器
コンテンツ供給機器
状態情報
登録条件署名
登録リスト署名
SAM62のID
ユーザのID
可
可
SAM62のID
なし
制限なし
×××
××××
レシーバ51の登録条件
対象SAM情報部
対象SAMID
SAM62のID
有効期限
××××
バージョン番号
××××
接続されている機器数
3
登録リスト

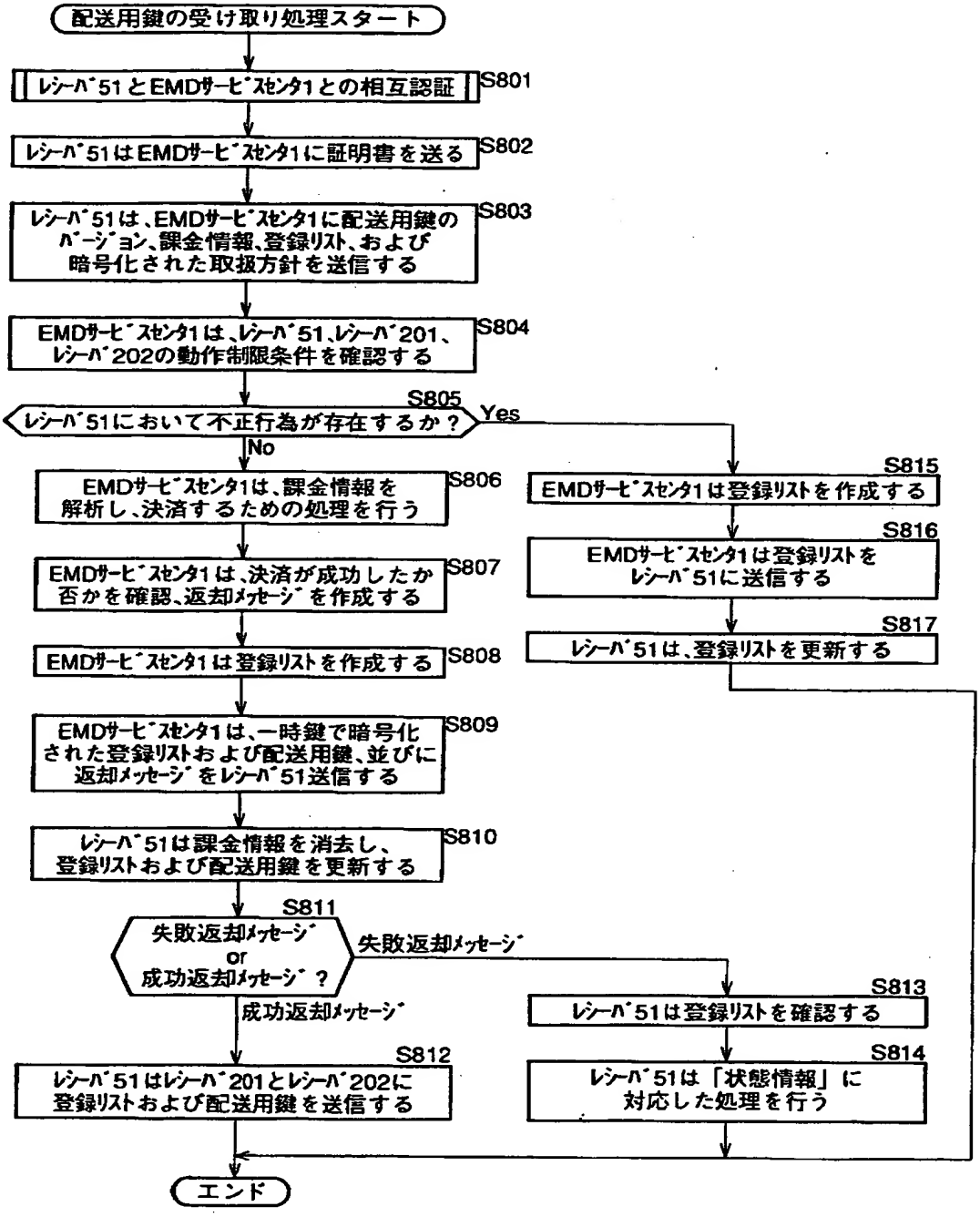
【図61】


レシーバ201、レシーバ202の
登録処理スタート
レシーバ51は、レシーバ201とレシーバ202の
情報を登録リストに書き加える
S701
レシーバ51とEMDサービスセンタ1との相互認証
S702
レシーバ51は、配送用鍵のバージョン、課金
情報、登録リスト、一時鍵で暗号化された
取扱方針をEMDサービスセンタ1に送信する
S703
EMDサービスセンタ1は、レシーバ201と
レシーバ202の動作制限条件を確認をする
S704
登録リストの作成
S705
EMDサービスセンタ1は、一時鍵で暗号化
した登録リストをレシーバ51に送信する
S706
レシーバ51は登録リストを記憶する
S707
リターン

【図62】


リスト部
SAM ID
ユーザ'ID
購入処理
課金処理
課金機器
コンテンツ供給機器
状態情報
登録条件署名
登録リスト署名
SAM62のID
SAM210のID
SAM220のID
ユーザ'のID
可
不可
不可
SAM62のID
SAM62のID
なし
なし
なし
SAM62のID
SAM210のID
制限なし
制限なし
制限なし
×××
×××
×××
××××
レシーバ'51の登録条件
対象SAM情報部
対象SAMID
SAM62のID
有効期限
××××
バージョン番号
××××
接続されている機器数
3

【図63】


配送用鍵の受け取り処理スタート
レシーバ51とEMDサービスセンタ1との相互認証
S801
レシーバ51はEMDサービスセンタ1に証明書を送る
S802
レシーバ51は、EMDサービスセンタ1に配送用鍵のバージョン、課金情報、登録リスト、および暗号化された取扱方針を送信する
S803
EMDサービスセンタ1は、レシーバ51、レシーバ201、レシーバ202の動作制限条件を確認する
S804
S805
レシーバ51において不正行為が存在するか？
Yes
No
EMDサービスセンタ1は、課金情報を解析し、決済するための処理を行う
S806
EMDサービスセンタ1は、決済が成功したか否かを確認、返却メッセージを作成する
S807
EMDサービスセンタ1は登録リストを作成する
S808
EMDサービスセンタ1は、一時鍵で暗号化された登録リストおよび配送用鍵、並びに返却メッセージをレシーバ51送信する
S809
レシーバ51は課金情報を消去し、登録リストおよび配送用鍵を更新する
S810
S811
失敗返却メッセージ or 成功返却メッセージ？
失敗返却メッセージ
成功返却メッセージ
S812
レシーバ51はレシーバ201とレシーバ202に登録リストおよび配送用鍵を送信する
S815
EMDサービスセンタ1は登録リストを作成する
S816
EMDサービスセンタ1は登録リストをレシーバ51に送信する
S817
レシーバ51は、登録リストを更新する
S813
レシーバ51は登録リストを確認する
S814
レシーバ51は「状態情報」に対応した処理を行う
エンド

【書類名】　　要約書

【要約】

【課題】　EMDシステムに登録された機器に、違反があったか否かを容易に確認することができる。

【解決手段】　EMDシステムに登録された各機器は、登録リストを保持する。例えば、課金処理が成功しなかった場合、その機器の登録リストの「状態情報」には、”制限あり”が設定される。この場合、その機器においては、すでに購入されたコンテンツの利用処理は実行されるが、新たなコンテンツを購入するための処理は実行されなくなる。また、その機器において、違反行為が発覚した場合、その機器の登録リストの「状態情報」には、”停止”が設定され、機器の動作が停止される。

【選択図】　　図５５

認定・付加情報

特許出願の番号	平成１１年　特許願　第１０３３３７号
受付番号	５９９００３３９６８５
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１１年　４月１５日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	000002185
【住所又は居所】	東京都品川区北品川６丁目７番３５号
【氏名又は名称】	ソニー株式会社

【代理人】　申請人

【識別番号】	100082131
【住所又は居所】	東京都新宿区西新宿７丁目５番８号　ＧＯＷＡ西新宿ビル６Ｆ　稲本国際特許事務所
【氏名又は名称】	稲本　義雄

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社